Concetti e procedure AMS Accelerate

Guida utente di AMS Accelerate

Version March 31, 2026

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Guida utente di AMS Accelerate: Concetti e procedure AMS Accelerate

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

I marchi e l'immagine commerciale di Amazon non possono essere utilizzati in relazione a prodotti o servizi che non siano di Amazon, in una qualsiasi modalità che possa causare confusione tra i clienti o in una qualsiasi modalità che denigri o discrediti Amazon. Tutti gli altri marchi non di proprietà di Amazon sono di proprietà dei rispettivi proprietari, che possono o meno essere affiliati, collegati o sponsorizzati da Amazon.

Table of Contents

Cos'è AMS Accelerate? 1
Piani operativi 1
Accelera il piano operativo 2
Piano operativo avanzato 2
Come funziona 2
Termini chiave 3
Descrizione del servizio 9
AWS Managed Services (AMS) Caratteristiche del piano operativo AMS Accelerate 10
Configurazioni supportate 13
Servizi supportati 15
Ruoli e responsabilità 19
Ambito delle modifiche apportate da AMS Accelerate 33
Sistemi operativi non supportati 34
Contatto ed escalation 35
Orari di contatto 36
Ore lavorative 36
Percorso di escalation 37
Inventario risorse 37
Controlli dell'infrastruttura 38
Nozioni di base 46
Onboarding 46
Prerequisiti di onboarding 46
Passaggio 1. Scoperta dell'account 49
Fase 2: Risorse per la gestione dell'onboarding 51
Fase 3. Funzionalità di onboarding con politiche predefinite 61
Fase 4. Personalizza le funzionalità 71
Uso delle console AMS 73
Modelli AMS 74
Come funzionano i pattern AMS 75
Modelli AMS 76
Configurazione automatica dell'istanza 79
Come funziona 79
Installazione automatica di SSM Agent 81
Modifiche automatiche alla configurazione delle ist 83

Offboard da AMS Accelerate ... 87
Effetti di offboarding ... 88
Offboarding con dipendenze ... 90
Ottenere assistenza per lo sbarco ... 90
Impostazioni notifiche ... 91
Assegnazione di tag ... 92
Tag ... 93
Cosa sono i tag? ... 93
Come funziona il tagging ... 94
Tag gestiti dal cliente ... 94
Tag con gestione accelerata ... 98
Tag forniti dal cliente ... 98
Strumenti di gestione dei tag ... 99
Resource Tagger ... 99
CloudFormation ... 120
Terraform ... 124
Segnalazioni di incidenti, richieste di assistenza e domande sulla fatturazione ... 126
Gestione degli incidenti ... 126
Cos'è la gestione degli incidenti? ... 127
Come funzionano la risposta e la risoluzione degli incidenti ... 128
Lavorare con gli incidenti ... 129
Gestione delle richieste di assistenza ... 132
Quando utilizzare una richiesta di assistenza ... 133
Come funziona la gestione delle richieste di assistenza ... 134
Creazione di una richiesta di servizio ... 135
Monitoraggio e aggiornamento di una richiesta di servizio ... 136
Gestione delle richieste di assistenza con l'API di supporto ... 137
Risposta a una richiesta di assistenza generata da AMS Accelerate ... 137
Report sugli incidenti e test delle richieste di assistenza ... 138
Domande sulla fatturazione ... 138
Gestione pianificata degli eventi ... 140
Criteri AMS PEM ... 140
Tipi di PEM ... 140
Il processo AMS PEM ... 140
PEM FAQs ... 141
Operazioni su richiesta ... 143

Richiedere AMS Operations On Demand ... 150
Apportare modifiche alle offerte Operations on Demand ... 151
Rapporti e opzioni ... 152
Report su richiesta ... 152
Rapporti sulla gestione degli host AMS ... 153
Report di AMS Backup ... 153
AWS Config Rapporto di controllo della conformità ... 156
Rapporto sulla configurazione delle risposte delle regole di configurazione di AMS Config ... 157
Incidenti evitati e monitoraggio dei report di Top Talker ... 160
Rapporto sui dettagli degli addebiti di fatturazione ... 161
Report di Trusted Remediator ... 163
Report self-service ... 166
Operazioni API interne ... 167
Rapporto sulle patch (giornaliero) ... 170
Rapporto di Backup (giornaliero) ... 180
Rapporto sull'incidente (settimanale) ... 184
Rapporto di fatturazione (mensile) ... 187
Rapporti aggregati ... 190
Dashboard di report self-service AMS ... 192
Policy di conservazione dei dati ... 200
Fuori bordo da SSR ... 200
Gestione degli accessi ... 202
Accesso alla console ... 202
Autorizzazioni per l'utilizzo delle funzionalità ... 202
Perché e quando accediamo al tuo account ... 217
Trigger di accesso ... 217
Accedi ai ruoli IAM ... 218
Come accediamo al tuo account ... 220
Come e quando usare root ... 221
Gestione della sicurezza ... 222
Utilizzo del documento SSM Log4j per scoprire le occorrenze ... 223
Monitoraggio della sicurezza dell'infrastruttura ... 224
Uso di ruoli collegati ai servizi ... 226
AWS politiche gestite ... 239
Protezione dei dati ... 248
Monitoraggio con Amazon Macie ... 248

Monitora con GuardDuty 249
Monitoraggio con il firewall DNS di Amazon Route 53 Resolver 250
Crittografia dei dati 252
AWS Identity and Access Management 252
Autenticazione con identità in AMS Accelerate 253
Gestione dell'accesso con policy 260
Risposta agli incidenti di sicurezza 261
Come funziona 262
Preparazione 262
Rilevamento 263
Analizzare 264
Contenere 265
Sradicare 267
Ripristino 268
Segnalazione successiva all'incidente 268
Runbook di risposta agli incidenti di sicurezza 269
Registrazione e monitoraggio degli eventi di sicurezza 274
Conformità di configurazione 275
Libreria AMS Config Rule 276
Risposte alle violazioni 301
Creazione di eccezioni alle regole 303
Ridurre AWS Config i costi 304
Risposte personalizzate ai risultati 304
Risposta agli incidenti 306
Risposta agli incidenti e onboarding 307
Resilienza 307
Controllo di sicurezza per sistemi end-of-support operativi 308
Best practice relative alla sicurezza 308
Revisioni di sicurezza delle richieste di modifica 308
Processo di gestione dei rischi per la sicurezza dei clienti 309
Standard tecnici AMS Accelerate 310
Controlli standard in AMS Accelerate 310
Modifiche che introducono rischi di sicurezza elevati o molto elevati nell'ambiente 325
Domande frequenti sulla sicurezza 327
Quando gli ingegneri operativi AMS accedono ai miei ambienti? 327
Quali ruoli assumono i tecnici operativi di AMS quando accedono ai miei account? 327

In che modo un tecnico operativo AMS accede al mio account? 328
Come posso tenere traccia delle modifiche apportate da AMS nei miei AWS account gestiti da AMS? 328
Quali sono i controlli di processo per l'accesso dei tecnici operativi AMS al mio account? 329
Come viene gestito l'accesso privilegiato? 329
I tecnici operativi di AMS utilizzano l'MFA? 330
Cosa succede al loro accesso quando un dipendente AMS lascia l'organizzazione o cambia ruolo lavorativo? 330
Quali controlli di accesso regolano l'accesso dei tecnici operativi AMS ai miei account? 330
In che modo AMS monitora l'accesso degli utenti root? 331
In che modo AMS risponde agli incidenti di sicurezza? 331
A quali certificazioni e framework standard del settore aderisce AMS? 331
Come posso accedere ai report più recenti sulla certificazione di sicurezza, sui framework e sulla conformità in materia? AWS 332
AMS condivide diagrammi di architettura di riferimento relativi a diversi aspetti delle funzionalità di AMS? 332
In che modo AMS monitora chi accede ai miei account e quali sono le esigenze aziendali di accesso? 333
I tecnici AMS hanno accesso ai miei dati archiviati in servizi di archiviazione AWS dati, come Amazon S3, Amazon RDS, DynamoDB e Amazon Redshift? 333
I tecnici AMS hanno accesso ai dati dei clienti archiviati in Amazon EBS, Amazon EFS e Amazon FSx? 334
In che modo l'accesso viene limitato o controllato per i ruoli di automazione che dispongono di privilegi elevati per i miei ambienti? 334
In che modo AMS implementa il principio del privilegio minimo come richiesto nel AWS Well-Architected Framework per i ruoli di automazione? 334
Quali sistemi di registrazione e monitoraggio vengono utilizzati per rilevare tentativi di accesso non autorizzati o attività sospette che coinvolgono ruoli di automazione? 334
Come vengono gestiti gli incidenti o le violazioni di sicurezza riguardanti l'infrastruttura di automazione e quali protocolli aiutano a rispondere e mitigare rapidamente? 335
Vengono effettuati regolarmente valutazioni di sicurezza, scansioni di vulnerabilità e test di penetrazione sull'infrastruttura di automazione? 335
In che modo l'accesso all'infrastruttura di automazione è limitato solo al personale autorizzato? 335
Quali misure vengono implementate per mantenere gli standard di sicurezza e prevenire accessi non autorizzati o violazioni dei dati nella pipeline di automazione? 336

Il rilevamento o il monitoraggio delle anomalie sono attivati per l'accesso o la registrazione degli audit per rilevare l'aumento dei privilegi o l'uso improprio degli accessi per avvisare in modo proattivo il team AMS? ... 336
Quali tipi di dati dei clienti vengono estratti dagli account gestiti da AMS e come vengono utilizzati e archiviati? ... 337
Monitoraggio e gestione degli eventi ... 338
Che cos'è il monitoraggio? ... 338
Come funziona il monitoraggio ... 339
Notifiche raggruppate di istanze EC2 ... 341
Notifica di avviso basata su tag ... 342
Avvisi dal monitoraggio di base in AMS ... 343
Notifiche di incidenti con riconoscimento delle applicazioni in AMS ... 366
Accedi AppRegistry e crea applicazioni ... 366
Crea tag per abilitare l'arricchimento dei casi ... 367
Personalizza la gravità dei casi di supporto AMS per le tue applicazioni ... 367
Rivedi le autorizzazioni richieste ... 369
Gestore degli allarmi ... 369
Come funziona Alarm Manager ... 370
Guida introduttiva ad Alarm Manager ... 371
Tag di Alarm Manager ... 372
Profili di configurazione di Alarm Manager ... 377
Creazione di allarmi aggiuntivi CloudWatch ... 395
Correzione automatica degli avvisi con AMS ... 395
Errore nel controllo dello stato di EC2: note sull'automazione della riparazione ... 402
Automazione della correzione dell'utilizzo dei volumi EC2 ... 402
Automazione della correzione degli eventi a basso livello di storage di Amazon RDS ... 403
Automazione della riparazione della capacità dei volumi ONTAP ... 404
Router per eventi AMS ... 404
Amazon EventBridge Managed Rules implementato da AMS ... 405
Creazione di regole gestite per AMS ... 407
Modifica delle regole gestite per AMS ... 408
Eliminazione delle regole gestite per AMS ... 408
Remediator affidabile ... 408
Vantaggi principali ... 408
Come funziona Trusted Remediator ... 409
Termini chiave ... 409

Inizia a usare Trusted Remediator 411
Raccomandazioni supportate per Compute Optimizer 413
Controlli supportati Trusted Advisor 417
Raccomandazioni CSPM di Security Hub supportate 477
Configura la correzione degli assegni 480
Workflow decisionale in modalità di esecuzione 484
Configura i tutorial di riparazione 484
Lavora con le riparazioni 487
Registri delle riparazioni 491
Integrazione con Quick 497
Best practice 499
FAQs 500
Monitoraggio e gestione degli incidenti per EKS 504
Che cos'è il monitoraggio e la gestione degli incidenti per Amazon EKS? 504
Come funzionano il monitoraggio e la gestione degli incidenti per Amazon EKS 505
Matrice di responsabilità AMS (RACI) 506
Avvisi di base 508
Avvisi e azioni 508
Requisiti 516
Onboarding 518
Fuori bordo 519
Gestione della continuità 521
Come funziona la gestione della continuità 521
Seleziona un piano di backup AMS 522
Piano di backup AMS predefinito 522
Piano di backup avanzato 523
Piano di backup per dati sensibili 524
Piano di backup AMS Accelerate Onboarding 524
Etichetta le tue risorse per il backup 525
Visualizza i backup nei vault AMS 526
Monitoraggio e reportistica per i backup 528
Gestione delle patch 529
Consigli per l'applicazione delle patch 530
Consigli sulla responsabilità delle patch 531
Linee guida per i team applicativi 531
Guida per i team addetti alle operazioni di sicurezza 532

Linee guida per i team di governance e conformità ... 532
Esempio di progettazione per un'applicazione Windows ad alta disponibilità ... 533
Consigli sulle patch FAQs ... 533
Crea una finestra di patch ... 534
Limiti della finestra di manutenzione delle patch ... 534
Crea la finestra di patch di Patch Tuesday: console AMS ... 536
Crea una finestra di patch: CloudFormation ... 537
Crea finestra di patch: console Systems Manager ... 538
Creazione della finestra di patch: Systems Manager CLI ... 540
Toppa con ganci ... 541
Agganci di patch AMS RACI ... 542
Crea documenti SSM per i patch hook ... 543
Configura la finestra di manutenzione delle patch AMS per utilizzare i documenti del comando SSM come patch hook AMS ... 543
Linea base delle patch AMS Accelerate ... 545
Linea di base della patch predefinita ... 545
Linea di base delle patch personalizzata ... 546
Autorizzazioni per l'applicazione di patch su richiesta ... 546
Comprendi le notifiche e gli errori delle patch ... 547
Richieste di assistenza patch e notifiche via e-mail ... 548
CloudWatch Notifiche di patch tramite Events ... 548
Indagine sugli errori delle patch ... 553
Ottimizzazione dei costi con AMS Resource Scheduler ... 554
Utilizzo delle risorse con Resource Scheduler ... 555
Onboarding Resource Scheduler ... 556
Personalizzazione di Resource Scheduler ... 557
Utilizzo di Resource Scheduler ... 558
Lavorare con periodi e pianificazioni ... 561
Tagging di risorse ... 567
Stimatore dei costi ... 567
Soppressore di allarmi ... 569
Gestione dei registri ... 570
Gestione dei log — AWS CloudTrail ... 570
Accesso e controllo dei log CloudTrail ... 572
Protezione e conservazione dei registri CloudTrail ... 572
Accesso ai log di Amazon EC2 ... 572

Conservazione dei log di Amazon EC2 573
Gestione dei log — Amazon EC2 573
Gestione dei log — Amazon VPC Flow Logs 574
Monitoraggio delle modifiche 576
Visualizzazione dei record delle modifiche 577
Interrogazioni predefinite 578
Modifica del filtro datetime nelle query 586
Esempi di query predefiniti 587
Modificare le autorizzazioni di registrazione 598
AWS Systems Manager in Accelerate 600
Documenti AMS Accelerate SSM disponibili 600
Versioni dei documenti AMS Accelerate SSM 600
Prezzi di Systems Manager 601
Cronologia dei documenti 602
Aggiornamenti precedenti 627
..... dclv

Cos'è AMS Accelerate?

Benvenuto in AMS Accelerate per Amazon Web Services (AWS). AMS Accelerate offre una gamma di servizi operativi per aiutarti a raggiungere l'eccellenza operativa su AWS. Che tu abbia appena iniziato a utilizzare il cloud, desideri ampliare il tuo team attuale o abbia bisogno di una soluzione operativa a lungo termine, Accelerate può aiutarti a raggiungere i tuoi obiettivi operativi nel cloud. Sfruttando Servizi AWS una libreria di automazioni, configurazioni e runbook, forniamo una soluzione end-to-end operativa per ambienti nuovi ed esistenti. AWS

Il servizio Accelerate sfrutta una suite di funzionalità Servizi AWS e funzionalità native per fornire un set completo di funzionalità di gestione dell'infrastruttura. All'interno di queste Servizi AWS, Accelerate crea e gestisce set curati di controlli di monitoraggio, barriere di rilevamento, automazioni e runbook per gestire l'infrastruttura in modo conforme e sicuro.

Argomenti

- Piani operativi AMS
- Utilizzo del piano operativo AMS Accelerate
- Termini chiave AMS
- Descrizione del servizio
- Funzionalità per sistemi operativi non supportati in Accelerate
- Contatto ed escalation
- Inventario risorse per Accelerate

Piani operativi AMS

AWS Managed Services (AMS) è disponibile con due piani operativi: AMS Accelerate e AMS Advanced. Un piano operativo offre un set specifico di funzionalità e prevede diversi livelli di servizio, capacità tecniche, requisiti, prezzi e restrizioni. I nostri piani operativi ti offrono la flessibilità necessaria per selezionare le capacità operative giuste per ciascuno dei tuoi AWS carichi di lavoro. Questa sezione descrive le capacità e le differenze, nonché le responsabilità, le caratteristiche e i vantaggi associati a ciascun piano, in modo che possiate capire quale piano operativo è il migliore per i vostri account.

Per un confronto dettagliato delle funzionalità dei due piani operativi, consulta AWS Managed Services Features.

Piano operativo AMS Accelerate

AMS Accelerate è il piano operativo AMS che ti aiuta a gestire l' day-to-dayinfrastruttura del tuo AWS ambiente nuovo o esistente. AMS Accelerate fornisce servizi operativi, come il monitoraggio, la gestione degli incidenti e la sicurezza. AMS Accelerate offre anche un componente aggiuntivo opzionale per carichi di lavoro EC2 basati su Amazon che richiedono patch regolari.

Con AMS Accelerate, sei Account AWS tu a decidere in che modo utilizzare AMS Accelerate, in quali regioni AWS desideri che AMS Accelerate operi, i componenti aggiuntivi necessari e gli accordi sui livelli di servizio (SLAs) di cui hai bisogno. Per maggiori dettagli, consulta Utilizzo del piano operativo di AMS Accelerate e descrizione del servizio.

Piano operativo AMS Advanced

AMS Advanced fornisce servizi per l'intero ciclo di vita per fornire, gestire e supportare l'infrastruttura. Oltre ai servizi operativi forniti da AMS Accelerate, AMS Advanced include anche servizi aggiuntivi, come la gestione delle landing zone, le modifiche e il provisioning dell'infrastruttura, la gestione degli accessi e la sicurezza degli endpoint.

AMS Advanced implementa una landing zone verso la quale migrare i AWS carichi di lavoro e ricevere i servizi operativi AMS. Le nostre zone di atterraggio gestite con più account sono preconfigurate con l'infrastruttura per facilitare l'autenticazione, la sicurezza, il networking e la registrazione.

AMS Advanced include anche un sistema di gestione delle modifiche e degli accessi che protegge i carichi di lavoro impedendo l'accesso non autorizzato o l'implementazione di modifiche rischiose all'infrastruttura. AWS I clienti devono creare una richiesta di modifica (RFC) utilizzando il nostro sistema di gestione delle modifiche per implementare la maggior parte delle modifiche nei vostri account AMS Advanced. Puoi creare modifiche automatiche a RFCs partire da una libreria di modifiche automatizzate verificate preventivamente dai nostri team di sicurezza e operativi oppure richiedi modifiche manuali che vengono riviste e implementate dal nostro team operativo se sono ritenute sicure e supportate da AMS Advanced.

Utilizzo del piano operativo AMS Accelerate

AMS Accelerate è il piano operativo AMS in grado di gestire l'infrastruttura AWS che supporta i carichi di lavoro. Sia che i tuoi carichi di lavoro siano già presenti in un account AWS o che tu stia pianificando di migrarne di nuovi, puoi beneficiare dei servizi operativi di AMS Accelerate come monitoraggio e avvisi, gestione degli incidenti, gestione della sicurezza e gestione dei backup, senza

dover effettuare una nuova migrazione, subire interruzioni o modificare il modo in cui utilizzi AWS. AMS Accelerate offre anche un componente aggiuntivo opzionale di patch per carichi di lavoro EC2 basati che richiedono patch regolari.

Con AMS Accelerate hai la libertà di usare, configurare e distribuire tutti i servizi AWS in modo nativo o con i tuoi strumenti preferiti. Puoi continuare a utilizzare i meccanismi di accesso e modifica esistenti mentre AMS applica costantemente pratiche collaudate che aiutano a scalare il tuo team, ottimizzare i costi, aumentare la sicurezza e l'efficienza e migliorare la resilienza.

Sebbene AMS Accelerate possa semplificare le tue operazioni, rimani responsabile dello sviluppo, dell'implementazione, del test, del tuning e della gestione delle applicazioni. AMS Accelerate apporta modifiche al tuo account solo a seguito di incidenti, allarmi, riparazioni e alcune richieste di assistenza. AMS Accelerate non fornisce risorse nell'account per tuo conto. AMS Accelerate fornisce assistenza per la risoluzione dei problemi di infrastruttura che influiscono sulle applicazioni, ma AMS Accelerate non accede né convalida le configurazioni delle applicazioni senza la vostra conoscenza e approvazione. I servizi e le modifiche di AMS Accelerate vengono forniti direttamente nella AWS console e APIs, quindi, puoi continuare a sfruttare i tuoi account esistenti con AWS le soluzioni AWS Marketplace disponibili. AMS Accelerate non modifica il codice nei infrastructure-as-code modelli (ad esempio i CloudFormation modelli), ma può indicare ai team le modifiche necessarie per seguire le migliori pratiche operative e di sicurezza.

Termini chiave AMS

- AMS Advanced: i servizi descritti nella sezione «Descrizione del servizio» della documentazione di AMS Advanced. Vedi Descrizione del servizio.
- Account AMS Advanced: AWS account che soddisfano sempre tutti i requisiti degli AMS Advanced Onboarding Requirements. Per informazioni sui vantaggi di AMS Advanced, sui case study e per contattare un addetto alle vendite, consulta AWS Managed Services.
- Account AMS Accelerate: AWS account che soddisfano in ogni momento tutti i requisiti degli AMS Accelerate Onboarding Requirements. Vedi Guida introduttiva ad AMS Accelerate.
- AWS Managed Services: AMS e/o AMS Accelerate.
- Account AWS Managed Services: gli account AMS e/o gli account AMS Accelerate.
- Raccomandazione critica: una raccomandazione emessa AWS tramite una richiesta di servizio che informa l'utente che è necessario intervenire per proteggersi da potenziali rischi o interruzioni delle risorse o del. Servizi AWS Se decidi di non seguire una raccomandazione critica entro la data specificata, sei l'unico responsabile di eventuali danni derivanti dalla tua decisione.

- Configurazione richiesta dal cliente: qualsiasi software, servizio o altra configurazione non identificata in:
  - Accelerazione: configurazioni supportate o AMS Accelerate; descrizione del servizio.
  - AMS Advanced: configurazioni supportate o AMS Advanced; descrizione del servizio.
- Comunicazione di un incidente: AMS comunica un Incidente all'utente o l'utente richiede un Incidente ad AMS tramite un Incidente creato nel Support Center for AMS Accelerate e nella console AMS per AMS. La console AMS Accelerate fornisce un riepilogo degli incidenti e delle richieste di assistenza sulla dashboard e collegamenti al Support Center per i dettagli.
- Ambiente gestito: gli account AMS Advanced e/o gli account AMS Accelerate gestiti da AMS.

  Per AMS Advanced, questi includono account multi-account landing zone (MALZ) e account single-account landing zone (SALZ).
- Data di inizio della fatturazione: il giorno lavorativo successivo alla AWS ricezione delle informazioni richieste nell'e-mail di onboarding di AWS Managed Services. L'e-mail di onboarding di AWS Managed Services si riferisce AWS all'e-mail inviata dall'utente per raccogliere le informazioni necessarie per attivare AWS Managed Services sui propri account.

  Per gli account registrati successivamente da te, la data di inizio della fatturazione è il giorno successivo all'invio da parte di AWS Managed Services di una notifica di attivazione di AWS Managed Services per l'account registrato. Una notifica di attivazione di AWS Managed Services si verifica quando:

  1. Concedi l'accesso a un AWS account compatibile e lo consegni a AWS Managed Services.
  2. AWS Managed Services progetta e crea l'account AWS Managed Services.
- Interruzione del servizio: puoi chiudere AWS Managed Services per tutti gli account AWS Managed Services o per uno specifico account AWS Managed Services per qualsiasi motivo fornendo un preavviso di AWS almeno 30 giorni tramite una richiesta di servizio. Alla data di cessazione del servizio, puoi:

  1. AWS ti cede i controlli di tutti gli account AWS Managed Services o degli account AWS Managed Services specificati, a seconda dei casi, oppure
  2. Le parti rimuovono i AWS Identity and Access Management ruoli che consentono AWS l'accesso da tutti gli account AWS Managed Services o dagli account AWS Managed Services specificati, a seconda dei casi.
- Data di cessazione del servizio: la data di cessazione del servizio è l'ultimo giorno del mese di calendario successivo alla fine del periodo di preavviso di cessazione richiesto di 30 giorni. Se la fine del periodo di disdetta richiesto cade dopo il ventesimo giorno del mese solare, la data

di cessazione del servizio è l'ultimo giorno del mese di calendario successivo. Di seguito sono riportati alcuni esempi di scenari relativi alle date di cessazione.

  - Se l'avviso di risoluzione viene fornito il 12 aprile, il preavviso di 30 giorni termina il 12 maggio. La data di cessazione del servizio è il 31 maggio.
  - Se viene fornito un avviso di risoluzione il 29 aprile, il preavviso di 30 giorni termina il 29 maggio. La data di cessazione del servizio è il 30 giugno.
- Fornitura di AWS Managed Services: ti AWS mette a disposizione e puoi accedere e utilizzare AWS Managed Services per ogni account AWS Managed Services a partire dalla data di inizio del servizio.
- Chiusura per determinati account AWS Managed Services: puoi chiudere AWS Managed Services per uno specifico account AWS Managed Services per qualsiasi motivo fornendo un AWS preavviso tramite una richiesta di servizio («Richiesta di terminazione dell'account AMS»).

Termini di gestione degli incidenti:

- Evento: un cambiamento nell'ambiente AMS.
- Avviso: ogni volta che un evento di un Servizio AWS operatore supportato supera una soglia e attiva un allarme, viene creato un avviso e viene inviato un avviso all'elenco dei contatti. Inoltre, viene creato un incidente nell'elenco degli incidenti.
- Incidente: un'interruzione o un peggioramento non pianificato delle prestazioni dell'ambiente AMS o di AWS Managed Services che provoca un impatto come riportato da AWS Managed Services o da te.
- Problema: causa principale condivisa di uno o più incidenti.
- Risoluzione di un incidente o risoluzione di un incidente:
  - AMS ha ripristinato tutti i servizi o le risorse AMS non disponibili relativi all'incidente riportandoli allo stato disponibile, oppure
  - AMS ha stabilito che gli stack o le risorse non disponibili non possono essere ripristinati allo stato disponibile, oppure
  - AMS ha avviato un ripristino dell'infrastruttura autorizzato dall'utente.
- Tempo di risposta agli incidenti: la differenza di tempo tra il momento in cui si crea un incidente e il momento in cui AMS fornisce una risposta iniziale tramite console, e-mail, centro di assistenza o telefono.
- Tempo di risoluzione dell'incidente: la differenza di tempo tra il momento in cui AMS o l'utente creano un incidente e il momento in cui l'incidente viene risolto.

- Priorità dell'incidente: in che modo AMS o l'utente assegna la priorità agli incidenti, definendoli come bassa, media o alta.
  - Bassa: un problema non critico del servizio AMS.
  - Medio: un servizio AWS all'interno dell'ambiente gestito è disponibile ma non funziona come previsto (secondo la descrizione del servizio applicabile).
  - Alto: (1) la console AMS o uno o più AMS APIs nell'ambiente gestito non sono disponibili; oppure (2) uno o più stack o risorse AMS all'interno dell'ambiente gestito non sono disponibili e l'indisponibilità impedisce all'applicazione di svolgere la propria funzione.

  AMS può riclassificare gli incidenti in base alle linee guida di cui sopra.
- Ripristino dell'infrastruttura: ridistribuzione degli stack esistenti, sulla base di modelli degli stack interessati, e avvio di un ripristino dei dati basato sull'ultimo punto di ripristino noto, se non diversamente specificato dall'utente, quando la risoluzione degli incidenti non è possibile.

Termini relativi all'infrastruttura:

- Ambiente di produzione gestito: un account cliente in cui risiedono le applicazioni di produzione del cliente.
- Ambiente non di produzione gestito: un account cliente che contiene solo applicazioni non di produzione, come applicazioni per lo sviluppo e il test.
- Stack AMS: un gruppo di una o più AWS risorse gestite da AMS come singola unità.
- Infrastruttura immutabile: un modello di manutenzione dell'infrastruttura tipico EC2 dei gruppi Amazon Auto Scaling ASGs () in cui i componenti dell'infrastruttura aggiornati (ad AWS esempio l'AMI) vengono sostituiti per ogni implementazione, anziché essere aggiornati sul posto. Il vantaggio dell'infrastruttura immutabile è che tutti i componenti rimangono in uno stato sincrono poiché vengono sempre generati dalla stessa base. L'immutabilità è indipendente da qualsiasi strumento o flusso di lavoro per la creazione dell'AMI.
- Infrastruttura mutabile: un modello di manutenzione dell'infrastruttura tipico per gli stack che non sono gruppi di Amazon EC2 Auto Scaling e contengono una singola istanza o solo poche istanze. Questo modello rappresenta più da vicino l'implementazione di sistema tradizionale, basata su hardware, in cui un sistema viene distribuito all'inizio del suo ciclo di vita e poi gli aggiornamenti vengono distribuiti su quel sistema nel tempo. Tutti gli aggiornamenti del sistema vengono applicati alle istanze singolarmente e possono comportare tempi di inattività del sistema (a seconda della configurazione dello stack) a causa del riavvio dell'applicazione o del sistema.

- Gruppi di sicurezza: firewall virtuali per l'istanza per controllare il traffico in entrata e in uscita. I gruppi di sicurezza operano a livello di istanza, non di sottorete. Pertanto, a ciascuna istanza di una sottorete del VPC potrebbe essere assegnato un set diverso di gruppi di sicurezza.
- Accordi sul livello di servizio (SLAs): parte dei contratti AMS con voi che definiscono il livello di servizio previsto.
- SLA non disponibile e indisponibilità:
  - Una richiesta API da te inviata che genera un errore.
  - Una richiesta di console inviata da te che genera una risposta HTTP 5xx (il server non è in grado di eseguire la richiesta).
  - Tutte Servizio AWS le offerte che costituiscono stack o risorse nell'infrastruttura gestita da AMS si trovano in uno stato di «interruzione del servizio», come indicato nella Service Health Dashboard.
  - L'indisponibilità derivante direttamente o indirettamente da un'esclusione di AMS non viene considerata nel determinare l'idoneità ai crediti di servizio. I servizi sono considerati disponibili a meno che non soddisfino i criteri per l'indisponibilità.
- Obiettivi del livello di servizio (SLOs): parte dei contratti AMS con l'utente che definiscono obiettivi di servizio specifici per i servizi AMS.

Termini di applicazione delle patch:

- Patch obbligatorie: aggiornamenti di sicurezza critici per risolvere problemi che potrebbero compromettere lo stato di sicurezza dell'ambiente o dell'account. Un «aggiornamento critico di sicurezza» è un aggiornamento di sicurezza classificato come «Critico» dal fornitore di un sistema operativo supportato da AMS.
- Patch annunciate o rilasciate: le patch vengono generalmente annunciate e rilasciate in base a una pianificazione. Le patch emergenti vengono annunciate quando viene scoperta la necessità della patch e, di solito, subito dopo, la patch viene rilasciata.
- Patch add-on: applicazione di patch basata su tag per le istanze AMS che sfrutta la funzionalità AWS Systems Manager (SSM) in modo da poter etichettare le istanze e applicare le patch a tali istanze utilizzando una linea di base e una finestra configurate dall'utente.
- Metodi di patch:
  - Patch sul posto: applicazione di patch che viene eseguita modificando le istanze esistenti.
  - Patch sostitutiva dell'AMI: patch che viene eseguita modificando il parametro di riferimento AMI di una configurazione di avvio del gruppo Auto EC2 Scaling esistente.

- Fornitore di patch (fornitori di sistemi operativi, terze parti): le patch vengono fornite dal fornitore o dall'organo direttivo dell'applicazione.
- Tipi di patch:
  - Aggiornamento critico di sicurezza (CSU): aggiornamento di sicurezza classificato come «critico» dal fornitore di un sistema operativo supportato.
  - Aggiornamento importante (UI): un aggiornamento di sicurezza classificato come «Importante» o un aggiornamento non relativo alla sicurezza classificato come «Critico» dal fornitore di un sistema operativo supportato.
  - Altro aggiornamento (OU): un aggiornamento del fornitore di un sistema operativo supportato che non è una CSU o un'interfaccia utente.
- Patch supportate: AMS supporta le patch a livello di sistema operativo. Gli aggiornamenti vengono rilasciati dal fornitore per correggere vulnerabilità di sicurezza o altri bug o per migliorare le prestazioni. Per un elenco delle configurazioni attualmente supportate OSs, consulta Support Configurations.

Termini di sicurezza:

- Detective Controls: una libreria di monitor creati o abilitati da AMS che forniscono una supervisione continua degli ambienti e dei carichi di lavoro gestiti dai clienti per configurazioni che non sono in linea con i controlli di sicurezza, operativi o dei clienti e intervengono informando i proprietari, modificando in modo proattivo o interrompendo le risorse.

Termini della richiesta di assistenza:

- Richiesta di assistenza: una richiesta da parte tua relativa a un'azione che desideri che AMS intraprenda per tuo conto.
- Notifica di avviso: avviso pubblicato da AMS nella pagina di elenco delle richieste di assistenza quando viene attivato un avviso AMS. Il contatto configurato per il tuo account viene inoltre avvisato tramite il metodo configurato (ad esempio, e-mail). Se hai dei tag di contatto sulle tue istanze/risorse e hai fornito il consenso al tuo cloud service delivery manager (CSDM) per le notifiche basate su tag, le informazioni di contatto (valore chiave) contenute nel tag vengono notificate anche per gli avvisi AMS automatici.
- Notifica di servizio: un avviso di AMS che viene pubblicato nella pagina dell'elenco delle richieste di assistenza.

Termini vari:

- Interfaccia AWS Managed Services: per AMS: la console AWS Managed Services Advanced, l'API AMS CM e Supporto l'API. Per AMS Accelerate: la Supporto console e Supporto l'API.
- Soddisfazione del cliente (CSAT): AMS CSAT viene informata con analisi approfondite, tra cui le valutazioni della corrispondenza dei casi su ogni caso o corrispondenza, sondaggi trimestrali e così via.
- DevOps: DevOps è una metodologia di sviluppo che promuove fortemente l'automazione e il monitoraggio in tutte le fasi. DevOps mira a cicli di sviluppo più brevi, a una maggiore frequenza di implementazione e a rilasci più affidabili, riunendo le funzioni di sviluppo e operazioni, tradizionalmente separate, su una base di automazione. Quando gli sviluppatori possono gestire le operazioni e le operazioni informano lo sviluppo, problemi e problemi vengono scoperti e risolti più rapidamente e gli obiettivi aziendali vengono raggiunti più rapidamente.
- ITIL: Information Technology Infrastructure Library (denominata ITIL) è un framework ITSM progettato per standardizzare il ciclo di vita dei servizi IT. ITIL è organizzato in cinque fasi che coprono il ciclo di vita dei servizi IT: strategia del servizio, progettazione del servizio, transizione del servizio, funzionamento del servizio e miglioramento del servizio.
- Gestione dei servizi IT (ITSM): un insieme di pratiche che allineano i servizi IT alle esigenze dell'azienda.
- Managed Monitoring Services (MMS): AMS gestisce il proprio sistema di monitoraggio, Managed Monitoring Service (MMS), che utilizza gli eventi AWS Health e aggrega i dati di CloudWatch Amazon e i dati di Servizi AWS altri, notificando agli operatori AMS (online 24 ore su 24, 7 giorni su 7) qualsiasi allarme creato tramite un argomento di Amazon Simple Notification Service (Amazon SNS).
- Namespace: quando crei policy IAM o lavori con Amazon Resource Names (ARNs), identifichi un utente Servizio AWS utilizzando uno spazio dei nomi. È possibile utilizzare gli spazi dei nomi quando si identificano azioni e risorse.

Descrizione del servizio

AMS Accelerate è un piano operativo del servizio AWS Managed Services per la gestione delle operazioni della tua AWS infrastruttura.

AWS Managed Services (AMS) Caratteristiche del piano operativo AMS Accelerate

AMS Accelerate offre le seguenti funzionalità:

- Gestione degli incidenti:

  La gestione degli incidenti è il processo utilizzato dal servizio AMS per rispondere agli incidenti segnalati.

  AMS Accelerate rileva e risponde in modo proattivo agli incidenti e assiste il team nella risoluzione dei problemi. Puoi contattare i tecnici operativi di AMS Accelerate 24 ore su 24, 7 giorni su 7 utilizzando AWS Support Center, con tempi di risposta che SLAs dipendono dal livello di risposta selezionato per il tuo account.
- Monitoraggio:

  Il monitoraggio è il processo utilizzato dal servizio AMS per tenere traccia delle risorse.

  Gli account registrati in AMS Accelerate sono configurati con una distribuzione di base di CloudWatch eventi e allarmi Amazon ottimizzati per ridurre il rumore e identificare un possibile incidente imminente. Dopo aver ricevuto gli avvisi, il team AMS si avvale di procedure automatizzate, personale e processi per riportare le risorse a uno stato ottimale e interagire con i team, se necessario, per fornire informazioni utili sul comportamento e su come prevenirlo. Se la riparazione fallisce, AMS avvia il processo di gestione degli incidenti. È possibile modificare le linee di base aggiornando il file di configurazione predefinito.
- Sicurezza:

  La gestione della sicurezza è il processo utilizzato dal servizio AMS per proteggere le risorse. AWS Managed Services protegge le tue risorse informative e aiuta a mantenere sicura la tua infrastruttura AWS utilizzando più controlli, tra cui AWS Config Rules e Amazon GuardDuty.

  AMS Accelerate gestisce una libreria di Regole di AWS Config azioni correttive per garantire che tutti gli account siano conformi agli standard di settore per la sicurezza e l'integrità operativa. Regole di AWS Config monitora continuamente la modifica della configurazione tra le risorse registrate. Se una modifica viola una delle condizioni delle regole, AMS ne segnala i risultati e consente di porre rimedio alle violazioni automaticamente o su richiesta, in base alla gravità della violazione. Regole di AWS Config facilitare la conformità agli standard stabiliti da: il Center for Internet Security (CIS), il National Institute of Standards and Technology (NIST) Cloud Security

Framework (CSF), l'Health Insurance Portability and Accountability Act (HIPAA) e il Payment Card Industry (PCI) Data Security Standard (DSS).

Inoltre, AMS Accelerate sfrutta Amazon GuardDuty per identificare attività potenzialmente non autorizzate o dannose nel tuo ambiente AWS. GuardDuty i risultati vengono monitorati 24 ore su 24, 7 giorni su 7 da AMS. AMS collabora con voi per comprendere l'impatto dei risultati e delle correzioni sulla base delle raccomandazioni delle migliori pratiche. AMS supporta anche Amazon Macie per proteggere i tuoi dati sensibili come informazioni sanitarie personali (PHI), informazioni di identificazione personale (PII) e dati finanziari. Infine, AMS monitora e classifica tutti gli eventi ALERT e BLOCK di Amazon Route 53 Resolver generati negli account gestiti per ispezionare ulteriormente il traffico di rete e potenziarne le capacità di rilevamento.

- Gestione delle patch:

  La gestione delle patch è il processo utilizzato dal servizio AMS per aggiornare le risorse.

  Per un AWS account con il componente aggiuntivo patch, AWS Managed Services applica e installa gli aggiornamenti dei fornitori alle istanze Amazon EC2 per i sistemi operativi supportati durante le finestre di manutenzione scelte. AMS crea un'istantanea dell'istanza prima dell'applicazione delle patch, monitora l'installazione della patch e notifica il risultato. Se la patch fallisce, AMS indaga sull'errore e consiglia una linea d'azione per risolvere il problema. In alternativa, AMS ripristina il rollback dell'istanza, se richiesto. AMS fornisce report sulla copertura della conformità delle patch e ti consiglia la linea d'azione consigliata per la tua azienda.

- Gestione del Backup:

  AMS utilizza la gestione dei backup per scattare istantanee delle risorse.

  AWS Managed Services crea, monitora e archivia istantanee per i AWS servizi supportati da. AWS Backup Puoi definire i piani di backup, la frequenza e il periodo di conservazione creando AWS Backup piani durante l'onboarding di account e applicazioni. I piani vengono associati alle risorse. AMS tiene traccia di tutti i processi di backup e, quando un processo di backup fallisce, avvisa il nostro team di eseguire una correzione. AMS sfrutta le istantanee per eseguire azioni di ripristino durante gli incidenti, se necessario. AMS fornisce un rapporto sulla copertura del backup e un rapporto sullo stato del backup.

- Gestione dei problemi:

  AMS esegue analisi delle tendenze per identificare e indagare sui problemi e identificarne la causa principale. I problemi vengono risolti con una soluzione alternativa o una soluzione permanente che impedisca il ripetersi di impatti futuri simili sui servizi. È possibile richiedere un rapporto post

incidente (PIR) per qualsiasi incidente «elevato», previa risoluzione. Il PIR analizza la causa principale e le azioni preventive intraprese, inclusa l'implementazione di misure preventive.

- Esperti designati:

  AMS Accelerate designa inoltre un Cloud Service Delivery Manager (CSDM) e un Cloud Architect (CA) per collaborare con la vostra organizzazione e promuovere l'eccellenza operativa e di sicurezza. Il CSDM e la CA ti forniscono indicazioni durante e dopo la configurazione e l'onboarding di AMS Accelerate, forniscono un rapporto mensile sui tuoi parametri operativi e collaborano con te per identificare potenziali risparmi sui costi utilizzando strumenti come AWS Cost Explorer, Cost and Usage Reports e. Trusted Advisor

- Strumenti operativi:

  AMS Accelerate può fornire operazioni continue per l'infrastruttura del carico di lavoro in AWS. I nostri servizi di patch, backup, monitoraggio e gestione degli incidenti dipendono dall'etichettatura delle risorse e dall'installazione e configurazione di AWS Systems Manager (SSM) e CloudWatch agenti sulle istanze Amazon EC2 con un profilo di istanza IAM che le autorizza a interagire con i servizi SSM e Amazon. CloudWatch AMS Accelerate fornisce strumenti come Resource Tagger per aiutarti a etichettare le tue risorse in base a regole e la configurazione automatica delle istanze per installare gli agenti richiesti nelle tue istanze Amazon EC2. Se segui pratiche di infrastruttura immutabili, puoi completare i prerequisiti direttamente nella console o nei modelli. infrastructure-as-code

- Ottimizzazione dei costi:

  AMS Resource Scheduler automatizza l'avvio e l'arresto delle istanze Amazon Elastic Compute Cloud (Amazon EC2), delle istanze Amazon Relational Database Service (Amazon RDS) e dei gruppi Amazon EC2 Auto Scaling. AMS Resource Scheduler ti aiuta a ridurre i costi operativi bloccando le risorse non utilizzate e riavviandole quando è necessaria la loro capacità.

- Registrazione e reportistica:

  AWS Managed Services aggrega e archivia i log generati a seguito di operazioni in CloudWatch CloudTrail, e Amazon VPC Flow Logs. La registrazione da AMS aiuta a velocizzare la risoluzione degli incidenti e gli audit di sistema. AMS Accelerate fornisce inoltre un rapporto mensile sull'assistenza che riassume i principali parametri prestazionali di AMS, tra cui un riepilogo e approfondimenti, metriche operative, risorse gestite, aderenza agli accordi sul livello di servizio AMS (SLA) e metriche finanziarie relative alla spesa, ai risparmi e all'ottimizzazione dei costi. I report vengono forniti dal cloud service delivery manager (CSDM) di AMS designato per te.

- Gestione delle richieste di assistenza:

Per richiedere informazioni sull'ambiente gestito, su AMS o sulle offerte di AWS servizi, invia le richieste di servizio utilizzando la console AMS Accelerate. Puoi inviare una richiesta di servizio per domande «pratiche» su AWS servizi e funzionalità o per richiedere servizi AMS aggiuntivi.

Tutti i clienti AMS Accelerate iniziano con la gestione degli incidenti, il monitoraggio, il monitoraggio della sicurezza, la registrazione dei registri, gli strumenti prerequisiti, la gestione dei backup e le funzionalità di reporting. Puoi aggiungere il componente aggiuntivo AMS Patch management a un prezzo aggiuntivo.

> **Note**
>
> Per un elenco delle funzionalità non supportate in AWS GovCloud (US), consulta In che modo AMS Accelerate si differenzia per AWS GovCloud (US)

Configurazioni supportate

AMS Accelerate supporta le seguenti configurazioni:

- Lingua: inglese.
- Regioni: consulta le AWS regioni supportate da AWS Managed Services nella pagina Web dei servizi AWS regionali.

> **Note**
>
> Le regioni AWS introdotte prima del 20 marzo 2019 sono considerate regioni «originali» e sono abilitate per impostazione predefinita. Le regioni introdotte dopo questa data sono regioni «Opt-in» e sono disabilitate per impostazione predefinita. Se il tuo account utilizza più regioni e hai effettuato l'onboarding di AMS Accelerate su un account con una regione «Opt-in» abilitata come regione predefinita, la funzione AMS Reporting è disponibile solo in quella regione. Se non imposti una regione predefinita, l'ultima regione che hai visitato è la tua regione predefinita.
> Per abilitare una regione, vedi Abilitazione di una regione. Per impostare una regione predefinita, vedi Scelta di una regione. Per un elenco dello stato di attivazione per ciascuna regione, consulta la sezione Regioni disponibili nella Amazon Elastic Compute Cloud User Guide.

- Architettura del sistema operativo (x86-64 o ARM64): qualsiasi architettura supportata da Systems Manager e. CloudWatch
- Sistemi operativi supportati:
  - AlmaLinux 8.3-8.9, 9.x (è supportato solo con l'architettura x86) AlmaLinux
  - Amazon Linux 2023
  - Amazon Linux 2 (data di fine del supporto AMS prevista per il 30 giugno 2026)
  - Oracle Linux 9.x, 8.x
  - Red Hat Enterprise Linux (RHEL) 9.x, 8.x
  - SUSE Linux Enterprise Server 15 SP6
  - SUSE Linux Enterprise Server per SAP 15 e versioni successive SP3
  - Microsoft Windows Server 2025, 2022, 2019, 2016
  - Ubuntu 20.04, 22.04, 24.04
- Sistemi operativi End of Support (EOS) supportati:

> **Note**
>
> I sistemi operativi End of Support (EOS) non rientrano nel periodo di supporto generale del produttore del sistema operativo e presentano un rischio maggiore per la sicurezza. I sistemi operativi EOS sono considerati configurazioni supportate solo se gli agenti richiesti da AMS supportano il sistema operativo e se sono soddisfatte le seguenti condizioni:
>
> 1. hai un supporto esteso con il fornitore del sistema operativo che ti consente di ricevere aggiornamenti, oppure
> 2. tutte le istanze che utilizzano un sistema operativo EOS seguono i controlli di sicurezza specificati da AMS nella Accelerate User Guide, oppure
> 3. rispettate tutti gli altri controlli di sicurezza compensativi richiesti da AMS.
>
> Nel caso in cui AMS non sia più in grado di supportare un sistema operativo EOS, AMS emette una raccomandazione critica per aggiornare il sistema operativo.
> Gli agenti richiesti da AMS possono includere, a titolo esemplificativo ma non esaustivo: AWS Systems Manager Amazon CloudWatch, l'agente Endpoint Security (EPS) e Active Directory (AD) Bridge (solo Linux).

  - Ubuntu Linux 18.04
  - SUSE Linux Enterprise Server 15 e SP3 SP4 SP5

- SUSE Linux Enterprise Server per SAP 15 SP2
- SUSE Linux Enterprise Server 12 SP5
- Servizio SUSE Linux Enterprise per SAP 12 SP5
- Microsoft Windows Server 2012/2012 R2
- Red Hat Enterprise Linux (RHEL) :7.x
- Oracle Linux 7.5-7.9

- Se lo utilizzi AWS Control Tower per gestire il tuo ambiente multi-account, assicurati di utilizzare la versione più recente di AWS Control Tower per garantire la compatibilità con Accelerate. Gli ambienti che utilizzano AWS Control Tower versioni precedenti alla 2.7 (rilasciate ad aprile 2021) non sono supportati. Per informazioni su come effettuare l'aggiornamento AWS Control Tower, consulta Update Your Landing Zone.

Servizi supportati

AWS Managed Services fornisce servizi di supporto alla gestione operativa per i seguenti AWS servizi. Ogni AWS servizio è distinto e, di conseguenza, il livello di supporto alla gestione operativa di AMS varia a seconda della natura e delle caratteristiche del AWS servizio sottostante. Se richiedi che AWS Managed Services fornisca servizi per qualsiasi software o servizio che non è espressamente identificato come supportato nel seguente elenco, tutti i servizi AWS Managed Services forniti per tali configurazioni richieste dal cliente verranno trattati come «Servizio beta» ai sensi dei Termini di servizio.

- Incidenti: tutti i servizi AWS
- Richiesta di assistenza: tutti i AWS servizi
- Applicazione di patch: Amazon EC2
- Backup e ripristino: tutti Servizi AWS supportati da. AWS Backup Per un elenco dei servizi supportati da AWS Backup, consulta Risorse AWS Backup supportate.
- Resource Scheduler: istanze Amazon Elastic Compute Cloud (Amazon EC2), gruppi Amazon Relational Database Service (Amazon RDS) e Amazon EC2 Auto Scaling
- Servizi monitorati per eventi operativi: controlli e Application Load Balancer supportati Trusted Advisor, Aurora, Amazon EC2, Elastic Load Balancing, Amazon NetApp for ONTAP, FSx FSx Amazon for Windows File Server, gateway NAT (un servizio Network Address Translation (NAT)), Amazon Health Dashboard Redshift OpenSearch, Amazon Relational Database Service (Amazon

RDS), VPN. Site-to-Site Per saperne di più su ciò che AMS Accelerate monitora come parte di un servizio, consulta Avvisi dal monitoraggio di base in AMS.

- Servizi monitorati dalle regole di configurazione di sicurezza: AWS Account, Macie GuardDuty, Amazon API Gateway,,,, AWS Certificate Manager, AWS Config, CloudTrail CloudWatch, Amazon AWS Database Migration Service DynamoDB AWS CodeBuild, Amazon EC2, Amazon, Amazon Elastic Block Store (Amazon EBS) ElastiCache, Amazon Elastic File System (Amazon EFS), Amazon Elastic Kubernetes Service (Amazon EKS), Elastic Load Balancing, Amazon Service, Amazon EMR, (AWS Identity and Access Management IAM), Amazon AWS Lambda Redshift, OpenSearch Amazon Relational Database Service, Amazon S3, AWS Key Management Service Amazon AI, Amazon SageMaker Gestione dei segreti AWS Simple Notification Service AWS Systems Manager, Amazon VPC (gruppo di sicurezza, volume, indirizzo IP elastico, connessione VPN, gateway Internet), Amazon VPC Flow Logs. Per ulteriori dettagli, consulta Conformità della configurazione in Acceler e Protezione dei dati in Accelerate. Puoi trovare ulteriori informazioni sulla sicurezza di AMS nella nostra Guida alla sicurezza privata a cui è possibile accedere tramite AWS Artifact, nella scheda Report, per AWS Managed Services.

> **Note**
>
> AMS Accelerate per la regione Asia Pacifico (Malesia) non supporta il monitoraggio con Amazon Macie, il monitoraggio e la gestione degli incidenti per Amazon EKS o il monitoraggio delle risorse Amazon EFS, FileSystem Amazon EC2 e Amazon EKS NatGateway Cluster. Inoltre, non supporta l'installazione automatica di SSM Agent.

> **Note**
>
> AMS Accelerate per la regione del Medio Oriente (EAU) supporta una serie di funzionalità specifiche, come descritto nella tabella seguente. L'accesso alla console dell'account AMS e alle istanze in questa regione è consentito esclusivamente dai trigger delle richieste di servizio in entrata. Per ulteriori informazioni sulla disponibilità di Accelerate nella regione del Medio Oriente (Emirati Arabi Uniti), consulta il tuo account manager o il AWS Cloud Service Delivery Manager (CSDM).

Funzionalità integrate di AMS Accelerate per la regione del Medio Oriente (Emirati Arabi Uniti)	Descrizione della funzionalità
Gestione degli incidenti	AMS fornisce risposte e assistenza agli incidenti per aiutare il tuo team a risolvere i problemi. Affinché AMS possa assistert i nella gestione degli incidenti, devi inviare una richiesta di assistenza. AMS non rileva o risponde in modo proattivo agli incidenti in questa regione.
Monitoraggio	Dopo aver ricevuto una richiesta di assistenz a da parte tua, AMS può aiutarti a ripristin are le risorse. AMS utilizza la riparazione, il personale e i processi automatizzati per riportare le risorse a uno stato ottimale. AMS non configura CloudWatch gli eventi e gli allarmi di base in questa regione. Se disponi di strumenti di monitoraggio esistenti, potrebbe essere disponibile un monitoraggio proattivo delle tue risorse basato sulla valutazione di Cloud Architect (CA) e CSDM.
Sicurezza	Dopo aver ricevuto una richiesta di assistenz a da parte tua, AMS può aiutarti a risolvere i problemi di sicurezza. AMS non implement a controlli di sicurezza come GuardDuty e/ o monitora Regole di AWS Config i risultati di sicurezza in questa regione. Se disponi di strumenti di sicurezza esistenti, potrebbe essere disponibile un monitoraggio proattivo della sicurezza basato sulla valutazione di CA e CSDM.
Gestione delle patch	AMS può applicare gli aggiornamenti dei fornitori alle istanze Amazon EC2 per i sistemi operativi supportati durante le finestre di

Funzionalità integrate di AMS Accelerate per la regione del Medio Oriente (Emirati Arabi Uniti)	Descrizione della funzionalità
	manutenzione selezionate e creare istantane e prima dell'applicazione delle patch. Affinché AMS possa assisterti nella gestione delle patch, devi inviare una richiesta di assistenza. Le notifiche e i report sulle patch AMS non sono disponibili in questa regione.
Gestione del Backup	AMS è in grado di creare e archiviare istantane e e fornire assistenza nella risoluzione dei backup. Servizi AWS AWS Backup Affinché AMS possa assisterti nella gestione dei backup, devi inviare una richiesta di assistenza. AMS non tiene traccia dei processi di backup in questa regione.
Esperti designati	AMS nomina un Cloud Architect (CA) e un Cloud Service Delivery Manager (CSDM) per collaborare con le organizzazioni dei clienti e promuovere l'eccellenza operativa e di sicurezza.
Gestione delle richieste di assistenza	Per richiedere informazioni sull'ambiente gestito, su AMS o sulle Servizio AWS offerte, invia le richieste di assistenza tramite la console AMS Accelerate. Puoi inviare una richiesta di servizio per domande «pratiche» Servizi AWS e sulle funzionalità o per richieder e i servizi AMS disponibili in questa regione, come descritto in questa tabella.

Ruoli e responsabilità

La matrice AMS Accelerate responsabile, responsabile, consultata e informata, o RACI, assegna la responsabilità principale al cliente o ad AMS per una serie di attività. La tabella descrive le tue responsabilità (il «Cliente») rispetto alle nostre («AMS Accelerate»).

La Ambito delle modifiche apportate da AMS Accelerate sezione elenca le circostanze specifiche in cui AMS è autorizzata ad apportare modifiche all'account dell'utente e alcuni tipi di modifiche che AMS non apporta mai.

Matrice RACI AMS Accelerate

AMS Accelerate gestisce la tua infrastruttura AWS. La tabella seguente fornisce una panoramica dei ruoli e delle responsabilità di te e di AMS Accelerate per le attività nel ciclo di vita di un'applicazione in esecuzione nell'ambiente gestito.

- R sta per Parte responsabile che fa il lavoro per raggiungere l'obiettivo.
- C sta per Consultato; una parte le cui opinioni vengono richieste, in genere come esperti in materia; e con la quale esiste una comunicazione bilaterale.
- I sta per Informed; una parte che viene informata sui progressi, spesso solo al completamento del compito.

> **Note**
>
> Alcune sezioni contengono «R» sia per AMS che per i clienti. Questo perché, nel modello di responsabilità AWS condivisa, sia AMS che i clienti assumono la responsabilità congiunta di rispondere ai problemi dell'infrastruttura e delle applicazioni.

Attività	Cliente	AWS Managed Services (AMS)
Modelli AMS		
Crea nuovi modelli	I	R

Attività	Cliente	AWS Managed Services (AMS)
Implementa e personalizza i modelli	R	C, I
Prova e rimuovi i modelli	R	I
Ciclo di vita delle applicazioni		
Sviluppo di applicazioni	R	I
Requisiti, analisi e progettazione dell'infrastruttura applicativa	R	I
Distribuzione delle applicazioni	R	I
Implementazione di risorse AWS	R	I
Monitoraggio dell'applicazione	R	I
Test/ottimizzazione delle applicazioni	R	I
Risolvi e risolvi i problemi relativi alle applicazioni	R	I
Risolvi e risolvi i problemi	R	I
Monitoraggio supportato per l'infrastruttura AWS	C	R
Risposta agli incidenti per problemi di rete AWS	C	R
Risposta agli incidenti per problemi relativi alle risorse AWS	C	R
Onboarding di account gestiti		
Concedi l'accesso all'account gestito AWS per il team e gli strumenti AMS	R	C
Implementa modifiche nell'account o nell'ambiente per consentire l'implementazione di strumenti nell'account. Ad esempio, modifiche alle politiche di controllo dei servizi (SCPs)	R	C

Attività	Cliente	AWS Managed Services (AMS)
Installa gli agenti SSM nelle istanze EC2	R	C
Installa e configura gli strumenti necessari per fornire i servizi AMS. Ad esempio, CloudWatch agenti, script per l'applicazione di patch, allarmi, registri e altro	I	R
Gestisci l'accesso e il ciclo di vita delle identità per gli ingegneri AMS	I	R
Raccogli tutti gli input necessari per configurare i servizi AMS. Ad esempio, durata, pianificazione e obiettivi delle finestre di manutenzione delle patch	R	I
Richiedi la configurazione dei servizi AMS e fornisci tutti gli input richiesti	R	I
Configura i servizi AMS come richiesto dal cliente. Ad esempio, finestre di manutenzione delle patch, resource tagger e alarm manager	C	R
Gestisci il ciclo di vita degli utenti e le relative autorizzazioni, per i servizi di directory locali, utilizzati per accedere agli account e alle istanze AWS	R	I
Consiglia l'ottimizzazione delle istanze riservate	I	R
Account di bordo su Trusted Remediator	C, IO	R
Gestione delle patch		
Raccogli tutti gli input necessari per configurare le finestre di manutenzi one delle patch, le linee di base delle patch e la destinazione	R	I
Richiedi la configurazione delle finestre e delle linee di base per la manutenzione delle patch e fornisci tutti gli input necessari	R	I
Configura le finestre di manutenzione delle patch, le linee di base delle patch e gli obiettivi come richiesto dal cliente	C	R

Attività	Cliente	AWS Managed Services (AMS)
Monitora gli aggiornamenti applicabili al sistema operativo supportato e al software preinstallato con il sistema operativo supportato per le istanze EC2	I	R
Segnala gli aggiornamenti mancanti del sistema operativo supportato e la copertura delle finestre di manutenzione	I	R
Scatta istantanee delle istanze prima di applicare gli aggiornamenti	I	R
Applica gli aggiornamenti alle istanze EC2 in base alla configurazione del cliente	I	R
Esamina gli aggiornamenti non riusciti alle istanze EC2	C	R
Aggiornamento AMIs e stack per i gruppi Auto-Scaling () ASGs	R	C
Applicare una patch al sistema operativo Windows e ai pacchetti Microsoft installati sul sistema operativo che sono regolati da Windows Update	I	R
Applicate le patch alle applicazioni installate, al software o alle dipendenze delle applicazioni non gestite da Windows Update	R	I
Applicate una patch al sistema operativo Linux e a qualsiasi pacchetto abilitato alla gestione dal gestore di pacchetti nativo del sistema operativo (ad esempio Yum, Apt, Zypper)	I	R
Patch le applicazioni installate, il software o le dipendenze delle applicazioni non gestite dal gestore di pacchetti nativo del sistema operativo Linux	R	I
Backup		
Raccogli tutti gli input necessari per configurare i piani di backup e indirizzare le risorse	R	I

Attività	Cliente	AWS Managed Services (AMS)
Richiedi la configurazione dei piani di Backup e fornisci tutti gli input richiesti	R	I
Configura i piani e gli obiettivi di backup come richiesto dal cliente	C	R
Specificate le pianificazioni di backup e le risorse di destinazione	R	I
Esegui backup per piano	I	R
Analizza i processi di backup non riusciti	I	R
Rapporto sullo stato dei processi di backup e sulla copertura dei backup	I	R
Convalida i backup	R	I
Richiedi il ripristino del backup per le risorse delle risorse dei servizi AWS supportate come parte della gestione degli incidenti	R	I
Esegui attività di ripristino del backup per le risorse dei servizi AWS supportati	I	R
Ripristina le applicazioni personalizzate o di terze parti interessate	R	I
Reti		
Fornitura e configurazione di Managed Account VPCs IGWs, Direct Connect e altri servizi di rete AWS	R	I
Configura e gestisci AWS Security Groups/NAT/NACL all'interno dell'account gestito	R	I
Configurazione e implementazione della rete all'interno della rete del cliente (ad esempio DirectConnect)	R	I
Configurazione e implementazione della rete all'interno della rete AWS	R	I

Attività	Cliente	AWS Managed Services (AMS)
Monitor definito da AMS per la sicurezza della rete, inclusi i gruppi di sicurezza	I	R
Configurazione e gestione dei log a livello di rete (log di flusso VPC e altro)	I	R
Registrazione di log		
Registra tutti i registri delle modifiche delle applicazioni	R	I
Registra i log delle modifiche dell'infrastruttura AWS	I	R
Abilita e aggrega l'audit trail di AWS	I	R
Registri aggregati dalle risorse AWS	I	R
Monitoraggio e correzione		
Raccogli tutti gli input necessari per configurare Alarm Manager, Resource Tagger e le soglie di allarme	R	I
Richiedi la configurazione di Alarm Manager e fornisci tutti gli input necessari	R	I
Configura Alarm Manager, Resource Tagger e le soglie di allarme come richiesto dal cliente.	C	R
Implementa le metriche e gli allarmi di CloudWatch base di AMS in base alla configurazione del cliente	I	R
Monitora le risorse AWS supportate utilizzando CloudWatch parametri e allarmi di base	I	R
Analizza gli avvisi provenienti dalle risorse AWS	C	R

Attività	Cliente	AWS Managed Services (AMS)
Risolvi gli avvisi in base a una configurazione definita o crea un incidente	I	R
Definisci, monitora e analizza i monitor specifici del cliente	R	I
Analizza gli avvisi derivanti dal monitoraggio delle applicazioni	R	C
Configura Trusted Advisor i controlli per la riparazione	R	C
Correggi automaticamente i controlli supportati Trusted Advisor	I	R
Correggi manualmente i controlli supportati Trusted Advisor	R	C
Segnala lo stato della riparazione	I	R
Risolvi gli errori di riparazione	R	C
Architettura di sicurezza		
Esamina le risorse e il codice AMS per individuare problemi di sicurezza e potenziali minacce	I	R
Implementa i controlli di sicurezza nelle risorse e nel codice AMS per mitigare i rischi di sicurezza	I	R
Abilita i servizi AWS supportati per la gestione della sicurezza dell'acco unt e delle relative risorse AWS	I	R
Gestisci le credenziali privilegiate per l'accesso all'account e al sistema operativo per gli ingegneri AMS	I	R
Gestione dei rischi di sicurezza		
Monitora i servizi AWS supportati per la gestione della sicurezza, come GuardDuty Macie	I	R

Attività	Cliente	AWS Managed Services (AMS)
Definisci e crea regole di Config definite da AMS per rilevare se le risorse AWS sono conformi alle best practice di sicurezza Center for Internet Security (CIS) e NIST.	I	R
Monitora le regole di Config definite da AMS	I	R
Segnala lo stato di conformità delle regole di Config	I	R
Definire un elenco di regole di Config richieste e correggerle	I	R
Valuta l'impatto della correzione delle regole di Config definite da AMS	R	I
Richiedi la correzione delle regole di Config definite da AMS nell'account AWS	R	I
Tieni traccia delle risorse esenti dalle regole di Config definite da AMS	R	I
Correggi le regole di Config definite da AMS supportate nell'account AWS	C	R
Correggi le regole di Config definite da AMS non supportate nell'account AWS	R	I
Definisci, monitora e analizza le regole di Config specifiche del cliente	R	I
Gestione degli incidenti		
Invia notifiche sugli incidenti rilevati da AMS nelle risorse AWS	I	R
Notifica gli incidenti nelle risorse AWS	R	I
Notifica gli incidenti per AWS le risorse basate sul monitoraggio	I	R
Gestisci i problemi di prestazioni e le interruzioni delle applicazioni	R	I
Classificate la priorità degli incidenti	I	R

Attività	Cliente	AWS Managed Services (AMS)
Fornisci una risposta agli incidenti	I	R
Fornisci la risoluzione degli incidenti o il ripristino dell'infrastruttura per le risorse con i backup disponibili	C	R
Risposta agli incidenti di sicurezza: preparazione		
Comunicazioni		
Fornisci e aggiorna i dati di contatto per la sicurezza dei clienti affinché AMS possa utilizzarli durante le notifiche di eventi di sicurezza e le escalation di sicurezza	R	I
Archivia e gestisci i dati di contatto per la sicurezza dei clienti forniti da utilizzare durante gli eventi di sicurezza e le escalation di sicurezza	C	R
Addestramento		
Fornisci al cliente la documentazione per supportare AMS durante il processo di risposta agli incidenti	I	R
Pratica la responsabilità condivisa durante i processi di risposta agli incidenti durante i Security Gamedays	R	R
Gestione delle risorse		
Configura la gestione della sicurezza supportata Servizi AWS per avvisi, correlazione degli avvisi, riduzione del rumore e regole aggiuntive	I	R
Mantieni un inventario completo delle AWS risorse (Amazon EC2, Amazon S3 ecc.), compresi i dettagli sul valore e la criticità di ogni risorsa per l'azienda. Queste informazioni saranno fondamentali per determinare una strategia di contenimento efficace	R	C
Utilizza i AWS tag per identificare risorse e carichi di lavoro	R	C

Attività	Cliente	AWS Managed Services (AMS)
Definisci e configura la conservazione e l'archiviazione dei log	I	R
Stabilisci una linea di base sicura definendo e applicando le politiche e le configurazioni di sicurezza dell'organizzazione per AWS account, servizi e gestione degli accessi	R	I
Risposta agli incidenti di sicurezza: rileva		
Registrazione, indicatori e monitoraggio		
Configura la registrazione e il monitoraggio per abilitare la gestione degli eventi, ad esempio, e degli account	I	R
Monitor supportato Servizi AWS per gli avvisi di sicurezza	I	R
Implementa e gestisci gli strumenti di sicurezza degli endpoint	R	I
Monitora la presenza di malware sulle istanze utilizzando la sicurezza degli endpoint	R	I
Informa il cliente degli eventi rilevati tramite messaggistica in uscita	I	R
Coordina le comunicazioni interne con gli stakeholder e gli aggiornamenti dei dirigenti per migliorare i tempi di risposta	R	I
Definisci, distribuisci e gestisci i servizi di rilevamento standard AMS (ad esempio, Amazon GuardDuty e AWS Config)	C	R
Registra i registri AWS delle modifiche all'infrastruttura	R	I
Abilita e configura la registrazione e il monitoraggio per abilitare la gestione degli eventi per l'applicazione	R	C

Attività	Cliente	AWS Managed Services (AMS)
Implementa e gestisci una lista di autorizzazioni, una lista di utenti non autorizzati e rilevamenti personalizzati sui servizi di AWS sicurezza supportati (ad esempio, Amazon) GuardDuty	R	R
Reportistica degli eventi di sicurezza		
Notifica ad AMS un'attività sospetta o un'indagine di sicurezza in corso	R	I
Notifica al cliente gli eventi e gli incidenti di sicurezza rilevati	I	R
Notifica l'evento pianificato che potrebbe attivare il processo di Security Incident Response	R	I
Security Incident Response - Analizza		
Indagine e analisi		
Esegui la risposta iniziale per l'avviso di sicurezza supportato generato da una fonte di rilevamento supportata	I	R
Valuta false/true gli aspetti positivi utilizzando i dati disponibili	R	R
Genera un'istantanea delle istanze interessate da condividere con il cliente, se necessario	I	R
Esegui attività di analisi forense come la catena di custodia, l'analisi del file system, l'analisi forense della memoria e l'analisi binaria	R	C
Raccogli i registri delle applicazioni per facilitare le indagini	R	I
Raccogli dati e registri per facilitare le indagini sugli avvisi di sicurezza	R	R
Partecipa alle SMEs indagini Servizi AWS di sicurezza	C	R

Attività	Cliente	AWS Managed Services (AMS)
Condividi i registri delle indagini fornite dall'assistenza Servizi AWS ai clienti durante un'indagine	I	R
Comunicazione		
Invia avvisi e notifiche dalle fonti di rilevamento AMS per le risorse gestite	I	R
Gestisci avvisi e notifiche per gli eventi di sicurezza delle applicazioni	R	I
Coinvolgi il punto di contatto per la sicurezza dei clienti durante un'indagi ne su un incidente di sicurezza	R	I
Risposta agli incidenti di sicurezza: contiene		
Strategia ed esecuzione di contenimento		
Valuta i rischi e decidi la strategia di contenimento, riconoscendo i potenziali impatti sui servizi	R	C
Effettua un backup dei sistemi interessati per ulteriori analisi	I	R
Contenete applicazioni e carichi di lavoro (tramite attività di configura zione o risposta specifiche dell'applicazione)	R	C
Definisci la strategia di contenimento in base all'incidente di sicurezza e alla risorsa interessata	I	R
Abilita la crittografia e l'archiviazione sicura dei backup point-in-time dei sistemi interessati	C	R
Esegui le azioni di contenimento supportate per AWS risorse tra cui istanze EC2, rete e IAM	I	R
Security Incident Response - Eradicate		

Attività	Cliente	AWS Managed Services (AMS)
Strategia ed esecuzione di eradicazione		
Definisci le opzioni di eradicazione in base all'incidente di sicurezza e alla risorsa interessata dai carichi di lavoro delle applicazioni dei clienti	C	R
Decidi la strategia di eradicazione concordata, i tempi di esecuzione dell'eradicazione e le conseguenze	R	I
Definisci le fasi di eradicazione in base all'incidente di sicurezza e alla risorsa interessata sui carichi di lavoro gestiti da AMS	C	R
Elimina le minacce e rafforza le AWS risorse, tra cui le istanze EC2, la rete e l'eliminazione dell'IAM	R	C
Elimina le minacce e rafforza le applicazioni e i carichi di lavoro (attraver so attività di configurazione o risposta specifiche dell'applicazione)	R	I
Risposta agli incidenti di sicurezza: ripristino		
Preparazione ed esecuzione del ripristino		
Configura i piani e gli obiettivi di backup come richiesto dal cliente	I	R
Rivedi i piani di backup per ripristinare i carichi di lavoro gestiti da AMS	R	I
Esegui attività di ripristino dei backup per le risorse supportate Servizi AWS	I	R
Esegui il backup dell'applicazione del cliente, della configurazione dell'APP e delle impostazioni di distribuzione e rivedi i piani di backup per ripristinare le applicazioni e i carichi di lavoro dei clienti dopo l'incidente	R	I
Ripristina le applicazioni e i carichi di lavoro dei clienti (tramite passaggi di ripristino specifici dell'applicazione)	R	I

Attività	Cliente	AWS Managed Services (AMS)
Risposta agli incidenti di sicurezza: rapporto successivo all'incidente		
Segnalazione successiva all'incidente		
Se necessario, condividete le lezioni apprese e le azioni da intraprendere con il cliente dopo l'incidente	I	R
Gestione dei problemi		
Correla gli incidenti per identificare i problemi	I	R
Esegui l'analisi della causa principale (RCA) dei problemi	I	R
Risolvere i problemi	I	R
Identifica e risolvi i problemi delle applicazioni	R	I
Gestione dei servizi		
Richiedi informazioni utilizzando le richieste di assistenza	R	I
Rispondi alle richieste di assistenza	I	R
Fornisci consigli per l'ottimizzazione dei costi	I	R
Prepara e fornisci un rapporto di assistenza mensile	I	R
Gestione delle modifiche		
Processi e strumenti di gestione delle modifiche per il provisioning e l'aggiornamento delle risorse nell'ambiente gestito	R	I
Manutenzione del calendario delle modifiche alle applicazioni	R	I
Avviso della prossima finestra di manutenzione	R	I

Attività	Cliente	AWS Managed Services (AMS)
Registra le modifiche apportate da AMS Operations	I	R
Ottimizzazione dei costi		
Raccogli tutti gli input necessari per configurare Resource Scheduler	R	I
Richiedi l'onboarding, la configurazione di Resource Scheduler e fornisci tutti gli input richiesti	R	I
Implementa Resource Scheduler in base alla configurazione del cliente	C, I	R
Disabilita e abilita il Resource Scheduler sull'account del cliente	R	C
Crea, elimina, descrivi e aggiorna le pianificazioni	C	R
Crea, elimina, descrivi e aggiorna i periodi	C	R
Analizza e risolvi i problemi con Resource Scheduler	I	R
Richiesta di offboarding del Resource Scheduler	R	I
Offboard del Resource Scheduler dall'account	C, IO	R

Ambito delle modifiche apportate da AMS Accelerate

AMS Accelerate apporta modifiche solo per gli scopi e le situazioni specifici descritti di seguito. AMS apporta modifiche solo a livello di infrastruttura, utilizzando la console o APIs. AMS non modifica mai i livelli di applicazione, controllo o dominio. Puoi vedere tutte le modifiche apportate da AMS (o da altri utenti) utilizzando il nostro set di query predefinite; a tale scopo, consulta. Monitoraggio delle modifiche nei tuoi account AMS Accelerate

AWS resources

AMS Accelerate distribuisce o aggiorna AWS le risorse solo nelle seguenti situazioni:

- Per distribuire e aggiornare gli strumenti e le risorse richiesti da AMS.
- Come parte del monitoraggio AMS, in risposta a eventi e allarmi.
- Risolvere i problemi di sicurezza nell'ambito di Risposte alle violazioni in Accelerate (rendere le risorse non conformi alle migliori pratiche di sicurezza).
- Durante la riparazione e il ripristino come parte della risposta a un incidente.
- Quando si risponde alle richieste dei clienti di configurare le funzionalità AMS, come le seguenti:
  - Gestore degli allarmi
  - Tagger di risorse
  - Linee di base delle patch e finestre di manutenzione
  - Pianificatore di risorse
  - Piani di backup

AMS Accelerate non distribuisce o aggiorna risorse al di fuori di queste situazioni. Se hai bisogno dell'aiuto di AMS per apportare modifiche in altre situazioni, prendi in considerazione l'utilizzo di Operations on Demand.

Software del sistema operativo

AMS Accelerate può apportare modifiche al software del sistema operativo in situazioni di indisponibilità tramite la risoluzione degli incidenti, come definito nel nostro accordo sul livello di servizio. AMS può anche apportare modifiche ai sistemi operativi come parte diConfigurazione automatica delle istanze in AMS Accelerate.

Codice e configurazione dell'applicazione

AMS Accelerate non modifica mai il codice (ad esempio, CloudFormation modelli AWS, altri infrastructure-as-code modelli o funzioni Lambda), ma può indicare ai team quali modifiche sono necessarie per seguire le migliori pratiche operative e di sicurezza. AMS Accelerate fornisce assistenza per la risoluzione dei problemi di infrastruttura che influiscono sulle applicazioni, ma AMS Accelerate non accede né convalida le configurazioni delle applicazioni.

Funzionalità per sistemi operativi non supportati in Accelerate

Un sistema operativo non supportato è qualsiasi sistema operativo non elencato in. Configurazioni supportate AMS considera le istanze con sistemi operativi non supportati come «configurazioni richieste dal cliente» soggette ai termini del AWS servizio Betas e Previews.

Il seguente set limitato di funzionalità AMS è disponibile per le istanze con sistemi operativi non supportati:

Funzionalità	Note
Gestione degli incidenti	AMS fornisce una risposta agli incidenti.
Gestione delle richieste di assistenza	AMS risponde alle richieste di assistenza.
Monitoraggio	AMS monitora e risponde ai controlli dello stato EC2 del sistema Amazon e ai controlli dello stato delle istanze. I controlli dello stato del sistema includono: perdita di connettività di rete, perdita di alimentazione del sistema, problemi software sull'host fisico e problemi hardware sull'host fisico che influiscono sulla raggiungibilità della rete. I controlli dello stato delle istanze includono: configura zione di rete o di avvio errata, memoria esaurita, file system danneggiato e kernel incompatibile.
Gestione della sicurezza	AMS monitora e risponde ai EC2 GuardDuty risultati e AWS Config alle regole di Amazon.
Gestione del Backup	AMS offre la gestione della continuità in Accelerate per EC2 l'utilizzo di AWS Backup piani e vault personalizzati con AMS.

Contatto ed escalation

Disponi di un cloud service delivery manager (CSDM) designato che fornisce assistenza consultiva in AMS Accelerate e ha una conoscenza dettagliata del caso d'uso e dell'architettura tecnologica per l'ambiente gestito. CSDMs collabora con account manager, account manager tecnici, architetti cloud AWS Managed Services (CAs) e architetti di soluzioni AWS (SAs), a seconda dei casi, per contribuire al lancio di nuovi progetti e fornire consigli sulle migliori pratiche durante lo sviluppo del software e i processi operativi. Il CSDM è il punto di contatto principale per AMS. Le principali responsabilità del vostro CSDM sono:

- Organizza e conduci riunioni mensili di revisione del servizio con i clienti.
- Fornisci dettagli sulla sicurezza, sugli aggiornamenti software per l'ambiente e sulle opportunità di ottimizzazione.
- Rispetta i tuoi requisiti, comprese le richieste di funzionalità per AMS Accelerate.
- Rispondi e risolvi le richieste di fatturazione e segnalazione dei servizi.
- Fornisci informazioni dettagliate per consigli finanziari e di ottimizzazione della capacità.

Orari di contatto

Puoi contattare AMS Accelerate per diversi motivi in momenti diversi.

Funzionalità	AMS Accelerate
	Livello Premium
Richiesta di assistenza	24/7
Gestione degli incidenti (P2-P3)	24/7
Backup e ripristino	24/7
Gestione delle patch	24/7
Monitoraggio e avvisi	24/7
Responsabile della fornitura di servizi cloud (CSDM)	Dal lunedì al venerdì: dalle 08:00 alle 17:00, orario lavorativo locale

Ore lavorative

Funzionalità	AMS Accelerate
	Livello Premium
Richiesta di assistenza	24/7
Gestione degli incidenti (P1)	24 ore su 24

Funzionalità	AMS Accelerate
	Livello Premium
Gestione degli incidenti (P2-P3)	24 ore su 24
Backup e ripristino	24/7
Gestione delle patch	24/7
Monitoraggio e avvisi	24/7
Responsabile della fornitura di servizi cloud (CSDM)	Dal lunedì al venerdì: dalle 09:00 alle 17:00, orario lavorativo locale

Percorso di escalation

AMS supporta i clienti con la gestione degli incidenti e la gestione delle richieste di assistenza, 24 ore al giorno, 7 giorni alla settimana, 365 giorni all'anno; in conformità con l'accordo sul livello di servizio AMS applicato all'account.

Per segnalare un problema di prestazioni del servizio AWS o AMS che influisce sull'ambiente gestito, utilizza la console AMS e invia un caso di incidente. Per informazioni dettagliate, vedi Invio di un incidente per Accelerate. Per informazioni generali sulla gestione degli incidenti con AMS, consultaGestione degli incidenti in AMS Accelerate.

Per richiedere informazioni o consigli o per richiedere servizi aggiuntivi ad AMS, utilizza la console AMS e invia una richiesta di assistenza. Per informazioni dettagliate, vedi Creazione di una richiesta di servizio in Accelerate. Per informazioni generali sulle richieste di assistenza AMS, consultaGestione delle richieste di assistenza in Accelerate.

Inventario risorse per Accelerate

Tutte le risorse che AMS Accelerate distribuisce ai tuoi Account AWS account sono elencate nel `resource_inventory.zip`file (foglio di calcolo Excel).

> **Note**
>
> Nella colonna Resource Name, il prefisso CFN: indica un ID CloudFormation logico anziché il nome di una risorsa. Questi vengono visualizzati per le risorse senza nome, ad esempio per le politiche dei bucket S3.

AMS implementa una serie di servizi come descritto in. Descrizione del servizio Il costo di implementazione è basso se implementati su un account vuoto, ma il costo aumenta con l'aumentare dell'utilizzo. Ad esempio, vengono creati registri e le regole di configurazione vengono richiamate quando le risorse cambiano.

Quando vengono apportate più modifiche alle regole di configurazione, è possibile attivare più invocazioni di conformità alla configurazione, con conseguenti costi più elevati. La stessa possibilità si applica ad Amazon CloudWatch utilizzato per il monitoraggio delle istanze: più granulare è il monitoraggio, maggiore è il costo del servizio. AWS Backup è un altro esempio. Se disponi di più backup archiviati o se hai periodi di conservazione più lunghi, stai utilizzando più spazio di archiviazione e il costo è più elevato.

Questi numeri sono difficili da prevedere. Durante la revisione aziendale mensile con il vostro cloud service delivery manager (CSDM), tenete traccia delle modifiche e lavorate per identificare le aree di opportunità per la riduzione dei costi.

Controlli dell'infrastruttura

AMS Accelerate utilizza risorse che potrebbero essere contrassegnate come configurazioni errate in determinati controlli. Tuttavia, queste configurazioni sono o compromessi intenzionali in termini di ottimizzazione dei costi o sono coperte da controlli di compensazione. AMS consiglia di utilizzare le informazioni contenute in questa documentazione per abilitare il controllo o per contrassegnare un'eccezione. AWS Security Hub

Argomenti

- Controlli di autoriparazione automatica del Security Hub in Accelerate
- Altri controlli del Security Hub in Accelerate

Controlli di autoriparazione automatica del Security Hub in Accelerate

I seguenti controlli di riparazione automatica sono disponibili in Accelerate.

Argomenti

- S3.7 - I bucket S3 per uso generico devono utilizzare la replica tra regioni
- S3.11 - I bucket S3 per uso generico devono avere le notifiche degli eventi abilitate
- S3.13 - I bucket S3 per uso generico devono avere configurazioni del ciclo di vita
- S3.15 - I bucket generici S3 devono avere Object Lock abilitato
- Config.1: AWS Config deve essere abilitato e utilizzare il ruolo collegato al servizio per la registrazione delle risorse

S3.7 - I bucket S3 per uso generico devono utilizzare la replica tra regioni

Risorse:

- arn:aws:s3<account_id>: :ams-a -alarmmanager- <region>
- <account_id>arn:aws:s3: :ams-a - - patch-data-reporting <region>
- <account_id><region>arn:aws:s3: :ams-a - - -audit patch-data-reporting
- arn:aws:s3::: - ams-config-recorder-bucket <account_id>
- <account_id>arn:aws:s3::: - -controllo ams-config-recorder-bucket

Nei bucket S3 utilizzati dai componenti dell'infrastruttura AMS non è abilitata la replica tra regioni, per ottimizzare i costi. L'abilitazione della replica tra regioni comporta costi di trasferimento dei dati per la replica dei dati tra regioni, oltre a costi di storage aggiuntivi nella regione di destinazione. Per i bucket che supportano le operazioni interne di AMS e non richiedono la ridondanza geografica per impostazione predefinita, la replica tra regioni aggiungerebbe costi continui significativi senza fornire i vantaggi necessari.

Poiché questi bucket archiviano dati operativi come la gestione degli allarmi, la segnalazione delle patch e la registrazione della configurazione all'interno di una singola regione, la replica tra regioni non è necessaria per le normali operazioni AMS. Tuttavia, AMS offre la possibilità di abilitare la replica interregionale su questi bucket in base ai requisiti specifici di disaster recovery o conformità. Contatta AMS se hai bisogno di assistenza nella configurazione della replica interregionale per il tuo caso d'uso.

S3.11 - I bucket S3 per uso generico devono avere le notifiche degli eventi abilitate

Risorse:

- <account_id>arn:aws:s3: :ams-a -alarmmanager- <region>

- <account_id>arn:aws:s3: :ams-a - - patch-data-reporting <region>
- <account_id><region>arn:aws:s3: :ams-a - - -audit patch-data-reporting
- arn:aws:s3::: - ams-config-recorder-bucket <account_id>
- <account_id>arn:aws:s3::: - -controllo ams-config-recorder-bucket

I bucket S3 utilizzati dai componenti dell'infrastruttura AMS non dispongono di notifiche di eventi abilitate per ottimizzare i costi. L'abilitazione delle notifiche di eventi S3 comporta costi per il meccanismo di consegna delle notifiche (come Amazon Simple Notification Service, SQS o AWS Lambda invocazioni), che possono aumentare a seconda del volume delle operazioni di S3. Per ulteriori informazioni, consulta i prezzi di Amazon SNS.

Poiché questi bucket supportano le operazioni interne di AMS e per impostazione predefinita non richiedono flussi di lavoro basati sugli eventi, non abbiamo abilitato le notifiche degli eventi per evitare costi inutili. Tuttavia, AMS offre la possibilità di abilitare le notifiche degli eventi su questi bucket in base a requisiti specifici di monitoraggio o automazione. Contatta AMS se hai bisogno di assistenza nella configurazione delle notifiche di eventi per il tuo caso d'uso.

S3.13 - I bucket S3 per uso generico devono avere configurazioni del ciclo di vita

Risorse:

- ams-config-recorder-bucketarn:aws:s3::: - <account_id>
- <account_id>arn:aws:s3::: - -controllo ams-config-recorder-bucket

Storicamente, il componente a cui appartengono queste risorse S3 non includeva queste configurazioni per motivi di efficienza in termini di costi per te. Tuttavia, AMS offre la possibilità di rimediare a questo controllo utilizzando la configurazione dell'utente. Contatta AMS se hai bisogno di assistenza in tal senso.

S3.15 - I bucket generici S3 devono avere Object Lock abilitato

Risorse:

- <account_id>arn:aws:s3: :ams-a -alarmmanager- <region>

I bucket S3 utilizzati dal sistema AMS Alarm Manager non hanno Object Lock abilitato per considerazioni relative all'efficienza dei costi. L'attivazione di Object Lock può aumentare i costi (sono

necessarie chiamate API aggiuntive con conseguente aumento CloudTrail dei dati) e la complessità operativa, in particolare per i bucket che richiedono aggiornamenti o eliminazioni frequenti degli oggetti nell'ambito delle normali operazioni. Tuttavia, è possibile abilitare manualmente Object Lock su questi bucket se i requisiti di conformità o conservazione dei dati richiedono questa funzionalità. Contatta AMS se hai bisogno di assistenza con questa configurazione.

Risorse:

- <account_id>arn:aws:s3: :ams-a - - patch-data-reporting <region>
- <account_id><region>arn:aws:s3: :ams-a - - -audit patch-data-reporting

Object Lock non può essere abilitato sui bucket and a causa delle limitazioni del servizio. `ams-a<AccountID>-patch-data-reporting-<Region>` `ams-a<AccountID>-patch-data-reporting-<Region>-audit` AWS Il patch-data-reporting bucket riceve i dati dall'inventario di Systems Manager tramite SSM Resource Data Sync, che è incompatibile con S3 Object Lock. Il bucket di controllo funge da destinazione per i log di accesso al server S3, che non può avere Object Lock abilitato. Per ulteriori informazioni, consulta Creazione di una sincronizzazione dei dati delle risorse per Inventory nella Guida per l'AWS Systems Manager utente. Questi vincoli AWS di servizio rendono Object Lock tecnicamente impossibile pur mantenendo le funzionalità richieste.

Config.1: AWS Config deve essere abilitato e utilizzare il ruolo collegato al servizio per la registrazione delle risorse

Risorse:

- Registratore Config

Durante l'onboarding, per impostazione predefinita, AMS utilizza il ruolo collegato AWS Config al servizio. `AWSServiceRoleForConfig` Tuttavia, questo controllo potrebbe fallire se sono stati forniti AWS Identity and Access Management ruoli personalizzati AWS Config anziché utilizzare il ruolo collegato al servizio per ridurre i costi. Sebbene i ruoli personalizzati possano funzionare, richiedono una gestione manuale delle policy e potrebbero non ricevere automaticamente gli aggiornamenti quando viene AWS Config aggiunto il supporto per nuovi tipi di risorse o funzionalità.

È possibile correggere automaticamente questo risultato aggiornando il AWS Config registratore per utilizzare il ruolo collegato al servizio. `AWSServiceRoleForConfig` Questa è la configurazione consigliata e si allinea alle best practice. AWS Per istruzioni dettagliate sull' AWS Config infrastruttura implementata da AMS, consulta Monitoraggio della sicurezza dell'infrastruttura.

Altri controlli del Security Hub in Accelerate

I seguenti controlli di compensazione sono disponibili in Accelerate.

Argomenti

- Lambda.3 - Le funzioni Lambda devono trovarsi in un VPC
- S3.17 - I bucket S3 per uso generico devono essere crittografati quando sono inattivi con AWS KMS keys
- KMS.2 - I responsabili IAM non dovrebbero disporre di politiche IAM in linea che consentano azioni di decrittografia su tutte le chiavi KMS
- S3.9 - I bucket S3 per uso generico devono avere la registrazione degli accessi al server abilitata
- EC2.6 - La registrazione del flusso VPC deve essere abilitata in tutti VPCs

Lambda.3 - Le funzioni Lambda devono trovarsi in un VPC

Risorse:

- AMSAlarmManagerDeploymentHandler
- AMSAlarmManagerOrphanedAlarmCleanup
- AMSAlarmManagerRemediation
- AMSAlarmManagerReporting
- AMSAlarmManagerTriggerEvaluation
- AMSAlarmManagerValidation
- AMSConfigExtensionDeploymentHandler
- AMSConfigFSXExtension
- AMSConfigOutpostExtension
- AMSConfigSyntheticCanaryExtension

Le AWS Lambda funzioni distribuite da AMS non comunicano con le risorse dei tuoi account. Pertanto, non richiedono interfacce di rete elastiche dedicate (ENIs) o il posizionamento di VPC. L'implementazione di queste funzioni al di fuori di un VPC riduce i costi e migliora la velocità di implementazione. Questo approccio non introduce alcun problema di sicurezza per la comunicazione tra le risorse. Poiché queste funzioni Lambda funzionano in modo indipendente e non accedono a

risorse basate su VPC, l'implementazione di VPC aggiunge complessità e costi non necessari senza fornire ulteriori vantaggi in termini di sicurezza.

S3.17 - I bucket S3 per uso generico devono essere crittografati quando sono inattivi con AWS KMS keys

Risorse:

- <account_id>arn:aws:s3: :ams-a -alarmmanager- <region>

I bucket Amazon Simple Storage Service utilizzati dal sistema AMS Alarm Manager utilizzano chiavi di crittografia gestite da Amazon (SSE-S3) anziché chiavi KMS gestite dal cliente (SSE-KMS). L'implementazione delle chiavi gestite dal cliente richiede la concessione di autorizzazioni esplicite ad AMS per utilizzare le chiavi KMS tramite politiche chiave. Ciò introduce complessità e rischi operativi aggiuntivi. L'utilizzo di questo controllo fornisce una crittografia avanzata a riposo, evitando al contempo costi aggiuntivi e complessità operative.

Se modificate le politiche delle chiavi, ruotate le chiavi in modo errato o eliminate o disabilitate accidentalmente le chiavi, il monitoraggio AMS fallisce immediatamente. Questa dipendenza dalla disponibilità delle chiavi gestita dal cliente compromette l'infrastruttura critica di monitoraggio e avviso di AMS. Potrebbe potenzialmente compromettere le funzionalità di monitoraggio in tempo reale, la trasmissione degli avvisi, la risposta agli incidenti e la visibilità dello stato del servizio.
Le chiavi di crittografia gestite da Amazon crittografano automaticamente i dati inattivi senza richiedere la gestione di policy chiave, pianificazioni di rotazione o autorizzazioni di accesso. Questa implementazione soddisfa i requisiti di crittografia mantenendo al contempo l'efficienza in termini di costi e la semplicità operativa per l'infrastruttura gestita. AMS

Risorse:

- <account_id><region>arn:aws:s3: :ams-a -cloudtrail-log- -audit

Il bucket di registrazione degli AWS CloudTrail audit non può utilizzare la crittografia a causa delle limitazioni del servizio. AWS KMS AWS I bucket S3 che fungono da destinazioni di registrazione degli accessi al server non devono avere la crittografia con chiave KMS abilitata. Per ulteriori informazioni, consulta Configurazione della crittografia predefinita e Risoluzione dei problemi di registrazione degli accessi al server nella Guida per l'utente di Amazon Simple Storage Service. L'attivazione della AWS KMS crittografia sui bucket di destinazione di registrazione può causare errori di registrazione e creare problemi operativi. Questo bucket utilizza invece la crittografia gestita da Amazon S3 (SSE-

S3). Ciò fornisce la crittografia a riposo mantenendo al contempo la compatibilità con la funzionalità di registrazione degli accessi al server S3.

KMS.2 - I responsabili IAM non dovrebbero disporre di politiche IAM in linea che consentano azioni di decrittografia su tutte le chiavi KMS

Risorse:

- Chiave KMS: alias/ams/patchreporting

La politica in linea contiene «Resource»: ["*"] in una policy chiave KMS, che è una politica basata sulle risorse allegata a una chiave KMS specifica (ams_ssm_inventory_bucket_kms_key). Le politiche chiave sono intrinsecamente limitate alla singola chiave e l'utilizzo di * nell'elemento Resource è una pratica standard poiché l'ambito della politica è già limitato dalla chiave stessa. AWS Per ulteriori informazioni, vedere Creating a key policy e Default key policy nella Developer Guide.AWS KMS keys Questa configurazione non presenta rischi per la sicurezza in quanto l'accesso è limitato a una singola chiave KMS, non a tutte le chiavi dell'account.

S3.9 - I bucket S3 per uso generico devono avere la registrazione degli accessi al server abilitata

Risorse:

- ams-config-recorder-bucket<account_id>- -controllo

Questi bucket S3 sono bucket di destinazione per la registrazione degli accessi per i bucket Recorder. AWS Config S3 sconsiglia di configurare la registrazione degli accessi su questi bucket in quanto genererebbe un ciclo infinito di registrazione, facendo aumentare inutilmente i costi. AWS Security Hub consiglia invece di eliminare i risultati delle risorse in questo scenario.

Correzione:

Dovresti sopprimere questo risultato per questi bucket interessati poiché i risultati non sono utili. Se non desideri eliminare i risultati, puoi facoltativamente configurare la registrazione automatica sul bucket. La registrazione automatica comporta il rischio che la registrazione venga rimossa se AMS aggiorna il bucket.

EC2.6 - La registrazione del flusso VPC deve essere abilitata in tutti VPCs

Risorse:

- Vpc predefinito alla creazione dell'account

Per impostazione predefinita, AMS non abilita i log di flusso VPC per il VPC predefinito.

Correzione:

È possibile correggere automaticamente il controllo aggiungendo la chiave/valore del `ams:managed=true` tag, cancellando lo stato della regola di configurazione ed eseguendo nuovamente la valutazione della regola. Il componente di riparazione automatica di AMS abilita i log di flusso VPC sul vpc.

Guida introduttiva ad AMS Accelerate

Se non disponi già di un account AWS Managed Services (AMS), inizia contattando un rappresentante di vendita di Amazon Web Services (AWS) utilizzando la nostra pagina AWS Managed Services - Contatta l'ufficio vendite.

Dopo esserti registrato a un AMS, il team di AMS Accelerate ti guida attraverso il seguente processo di onboarding per ciascuno dei tuoi. Account AWS

Consulta il set di funzionalità qui: AWS Managed Services Features

> **Note**
>
> AMS GovCloud Accelerate supporta le regioni. Se il tuo servizio risiederà in un AWS GovCloud (US) Region, consulta anche Guida introduttiva a AWS GovCloud (US).

Procedura di registrazione dell'account per Accelerate

L'onboarding di un account in AMS Accelerate prevede quattro fasi.

1. Passaggio 1. Identificazione degli account in Accelerate valuta lo stato attuale del tuo account e identifica gli ostacoli tecnici all'onboarding del tuo account.
2. Fase 2: Risorse di gestione dell'onboarding in Accelerate ti chiede di accettare i termini e le condizioni e di creare un ruolo di onboarding per gli architetti cloud di AMS Accelerate (CAs), che ti assisteranno nella definizione di una base di sicurezza e nella risoluzione dei problemi, se necessario.
3. Fase 3. Integrazione delle funzionalità AMS con policy predefinite per le funzionalità di Accelerate, come il monitoraggio, l'applicazione di patch e il backup.
4. Fase 4. Personalizza le funzionalità in Accelerate assicura che le risorse, incluse le EC2 istanze, siano configurate correttamente per l'applicazione.

Accelera i prerequisiti per l'onboarding

Prima di iniziare il processo di onboarding, è importante comprendere le dipendenze tecniche su cui si basano i componenti Accelerate.

> **Note**
>
> Per utilizzare AMS Accelerate, devi avere uno dei due Supporto piani supportati: Enterprise On-Ramp o Enterprise. I piani Developer e Business non sono idonei per qualificarsi per AMS Accelerate. Per saperne di più sui diversi piani, consulta Confronta Supporto i piani.

Endpoint VPC AMS Accelerate

Un endpoint VPC consente connessioni private tra il tuo VPC e i servizi supportati AWS e i servizi endpoint VPC forniti da. AWS Se devi filtrare la connettività Internet in uscita, configura i seguenti endpoint del servizio VPC per garantire che AMS Accelerate abbia la connettività con le sue dipendenze di servizio.

> **Note**
>
> Nell'elenco seguente, *region* rappresenta l'identificatore di una AWS regione, ad esempio `us-east-2` per la regione Stati Uniti orientali (Ohio).

```
com.amazonaws.region.logs
com.amazonaws.region.monitoring
com.amazonaws.region.ec2
com.amazonaws.region.ec2messages
com.amazonaws.region.ssm
com.amazonaws.region.ssmmessages
com.amazonaws.region.s3
com.amazonaws.region.events
```

Per informazioni su come configurare gli endpoint VPC di AWS, consulta Endpoint VPC.

> **Note**
>
> Se stai creando endpoint VPC nel tuo account per tutti i servizi sopra menzionati, consulta questo modello di esempio. CloudFormation Puoi aggiornare questo modello e rimuovere o aggiungere la definizione degli endpoint VPC secondo il tuo caso d'uso.

Connettività Internet in uscita in Accelerate

1. Scarica egressMgmt.zip.
2. Apri il file **ams-egress.json**.
3. Trovalo URLs nelle proprietà JSON:
   - `WindowsPatching`
   - `RedHatPatching`
   - `AmazonLinuxPatching`
   - `EPELRepository`
4. Consenti l'accesso a questi URLs.

Test della connettività in uscita in Accelerate

Verifica la connettività in uscita utilizzando uno dei seguenti metodi.

> **Note**
>
> Prima di eseguire lo script/comando, sostituisci il rosso *region* con l'identificatore della regione, ad esempio. `us-east-1`

Script di Windows PowerShell

```
$region = 'region'
@('logs','monitoring','ec2','ec2messages','ssm','ssmmessages','s3','events') | `
ForEach-Object { `
Test-NetConnection ("$_" + '.' + "$region" + '.amazonaws.com') -Port 443 } | `
Format-Table ComputerName,RemotePort,RemoteAddress,PingSucceeded,TcpTestSucceeded -
AutoSize
```

Comando Linux

```
for endpoint in logs monitoring ec2 ec2messages ssm ssmmessages s3 events; do nc -zv
 $endpoint.region.amazonaws.com 443; done
```

Amazon EC2 Systems Manager in Accelerate

È necessario installare l' AWS Systems Manager agente (agente SSM) su tutte le EC2 istanze che si desidera che AMS gestisca. È inoltre necessario aggiungere le autorizzazioni del bucket richieste dall'agente SSM. Per una panoramica che include Amazon EC2, consultaFase 3. Integrazione delle funzionalità AMS con policy predefinite.

IAM in Accelerate

Per consentire agli utenti di leggere e configurare le funzionalità di AMS Accelerate, come l'accesso alla console AMS o la configurazione dei backup, è necessario concedere autorizzazioni esplicite in AWS Identity and Access Management (IAM) per eseguire tali azioni. Per esempio le politiche IAM, consulta Autorizzazioni all'uso delle funzionalità AMS.

Passaggio 1. Identificazione degli account in Accelerate

AMS collabora con te durante l'individuazione dell'account per valutare lo stato attuale del tuo account e identificare gli ostacoli tecnici all'onboarding del tuo account. AMS non fornisce servizi operativi durante la fase di scoperta dell'account. AMS utilizza il ruolo `AWSServiceRoleForSupport` collegato ai servizi per identificare i blocchi tecnici e quindi collabora con te per porvi rimedio, prima di passare alla fase di onboarding a livello di account.

Processo di scoperta degli account in Accelerate

Per aiutarti nell'analisi e nell'individuazione del tuo account, AMS esegue controlli operativi per identificare i blocchi tecnici tramite chiamate API di sola lettura. Dopo l'onboarding dell'account su AMS, questi controlli vengono eseguiti su richiesta per mantenere la situazione dell'account. AMS collabora con te per correggere eventuali criticità associate a questi controlli quando necessario. AMS utilizza i seguenti controlli operativi e azioni API di sola lettura come parte di Account Discovery:

Controllo operativo	Scopo	AWS Chiamate API utilizzate
AWS Control Tower Valutazione della versione	Identifica la AWS Control Tower versione per assicurarsi che sia la versione minima supportata per l'onboarding di. Account AWS	• `ControlTower:GetLandingZone` • `ControlTower:ListEnabledControls`

Controllo operativo	Scopo	AWS Chiamate API utilizzate
		• `ControlTower:ListLandingZones`
AWS CloudTrail Valutazione	Identifica i AWS CloudTrail percorsi e le relative configurazioni per l'onboarding per ridurre Account AWS al minimo i costi dei percorsi. CloudTrail	• `CloudTrail:GetTrail` • `CloudTrail:ListTrails` • `S3:GetBucketOwnershipControls` • `S3:GetBucketPolicy` • `KMS:GetKeyPolicy` • `CloudTrail:GetEventSelectors` • `S3:GetBucketLogging` • `S3: GetBucketLifecycleConfiguration` • `S3: GetBucketEncryption`
CloudFormation Valutazione del gancio	Identifica i CloudFormation fattori di onboarding Account AWS che bloccano l'implementazione del servizio AMS nel tuo. Account AWS	• `CloudFormation:ListTypes`
Valutazione delle istanze Amazon EC2	Identifica le istanze EC2 del tuo sistema Account AWS che non utilizzano AWS Systems Manager Agent (SSM Agent) e che non sono supportate da AMS.	• `EC2:DescribeInstances` • `EC2:DescribeImages` • `SSM:DescribeInstanceInformation`

AMS Accelerate segue le migliori pratiche del settore per soddisfare e mantenere l'idoneità alla conformità. L'accesso di AMS Accelerate Discovery al tuo account viene registrato AWS CloudTrail tramite il ruolo collegato al AWSServiceRoleForSupport servizio. Questo aiuta a soddisfare i requisiti di monitoraggio e controllo. Per informazioni in merito AWS CloudTrail, consulta la Guida per l'AWS CloudTrail utente.

Fase 2: Risorse di gestione dell'onboarding in Accelerate

Questa è una panoramica del processo di onboarding delle risorse di gestione.

Accetti i termini

Il tuo gestore di distribuzione dei servizi cloud (CSDM) ti guida attraverso il processo di accettazione. Devi accettare i Termini e condizioni Regioni AWS, selezionare i componenti aggiuntivi e un contratto sul livello di servizio (SLA).

Concedi le autorizzazioni ai ruoli AMS

Devi concedere l'accesso ai processi AMS e al tuo Cloud Architect. Puoi farlo creando uno CloudFormation stack per ogni ruolo. Vedi Il modello per creare ruoli AMS e poiCrea `aws_managedservices_onboarding_role` con CloudFormation for Accelerate. Per ulteriori dettagli, consulta Gestione degli accessi in AMS Accelerate.

AMS esamina la tua configurazione

Il tuo Cloud Architect (CA) cerca anche possibili problemi di configurazione nel tuo account, come le politiche di controllo dei servizi (SCPs), e i problemi di sicurezza che potrebbero impedire ad AMS di implementare gli strumenti e le risorse richiesti da AMS. La tua CA collabora con te per aiutarti a correggere i risultati e rimuovere eventuali ostacoli all'implementazione degli strumenti e delle risorse AMS.

AMS esamina le configurazioni dei percorsi AWS CloudTrail

Il tuo Cloud Architect (CA) esaminerà le configurazioni del CloudTrail percorso e confermerà se desideri che AMS distribuisca un CloudTrail trail globale o integri Accelerate con le risorse del tuo CloudTrail account o dell'organizzazione. Se scegli di integrare Accelerate con il tuo CloudTrail trail, il tuo CA ti guiderà attraverso gli aggiornamenti necessari alle configurazioni per le tue CloudTrail risorse trail.

AMS distribuisce risorse di gestione

Il team AMS utilizza strumenti e AWS risorse per fornire i diversi servizi di AMS Accelerate. Una volta completato, AMS ha creato l'account AWS Managed Services e AMS ti notifica che il tuo account è attivo.

Questo conclude la fase delle risorse di gestione dell'onboarding. Puoi procedere direttamente alla fase successiva del processo di onboarding:. Fase 3. Integrazione delle funzionalità AMS con policy predefinite

> **Note**
>
> Ora che il tuo account è attivo, hai la possibilità di eseguire una di queste attività:
>
> - Crea incidenti e richieste di assistenza per l' AWS infrastruttura utilizzando la console Support Center. Per informazioni, consulta Segnalazioni di incidenti, richieste di assistenza e domande di fatturazione in AMS Accelerate.
> - Visualizza lo stato di conformità nel tuo account delle AWS Config regole implementate da AMS,. Conformità della configurazione in Acceler
> - Individua GuardDuty e analizza i risultati di Macie (opzionale). Per informazioni, consulta Monitora con GuardDuty.
> - Registri di accesso e controllo CloudTrail
> - Tieni traccia delle modifiche nel tuo account AMS Accelerate. Per informazioni, consulta Monitoraggio delle modifiche nei tuoi account AMS Accelerate.
> - Usa Resource Tagger per creare tag. Per informazioni, consulta Accelera Resource Tagger.
> - Richiedi patch, backup e AWS Config report. Per informazioni, consulta Rapporti e opzioni.

Rivedi e aggiorna le configurazioni per consentire ad AMS Accelerate di utilizzare il tuo trail CloudTrail

AMS Accelerate si affida alla AWS CloudTrail registrazione per gestire gli audit e la conformità per tutte le risorse del tuo account. Durante l'onboarding, scegli se Accelerate distribuisca un CloudTrail percorso nella tua AWS regione principale o utilizzi gli eventi generati dal tuo account o percorso organizzativo esistente. CloudTrail Se sul tuo account non è configurato un trail, Accelerate implementerà un percorso gestito CloudTrail durante l'onboarding.

> **Important**
>
> CloudTrail la configurazione della gestione dei registri è richiesta solo quando scegli di integrare AMS Accelerate con il tuo CloudTrail account o Organization trail.

Rivedi le configurazioni dei CloudTrail percorsi, la policy sui bucket di Amazon S3 AWS KMS e la politica chiave per CloudTrail la destinazione di consegna degli eventi con Cloud Architect (CA)

Prima che Accelerate possa utilizzare il tuo CloudTrail trail, devi collaborare con Cloud Architect (CA) per rivedere e aggiornare le configurazioni per soddisfare i requisiti di Accelerate. Se scegli di integrare Accelerate con la tua CloudTrail organizzazione, il tuo CA collaborerà con te per aggiornare il bucket Amazon S3 della destinazione di distribuzione CloudTrail degli eventi e le politiche AWS KMS chiave per abilitare le query su più account dal tuo account Accelerate. Il tuo bucket Amazon S3 può trovarsi in un account gestito da Accelerate o in un account che gestisci tu. Durante l'onboarding, Accelerate verifica che sia possibile effettuare query verso la destinazione di consegna degli eventi di tracciamento CloudTrail dell'organizzazione e sospende l'onboarding se le richieste non riescono. Collaborate con la vostra CA per correggere queste configurazioni in modo che l'onboarding possa riprendere.

Rivedi e aggiorna le configurazioni CloudTrail dell'account o dell'organizzazione

Le seguenti configurazioni sono necessarie per integrare Accelerate CloudTrail log management, il tuo CloudTrail account o le risorse Organization trail:

- Il CloudTrail percorso è configurato per registrare tutti Regioni AWS gli eventi.
- Il tuo CloudTrail percorso ha gli eventi di servizio globali abilitati.
- Il percorso dell' CloudTrail account o dell'organizzazione registra tutti gli eventi di gestione, inclusi gli eventi di lettura e scrittura, AWS KMS e la registrazione degli eventi di Amazon RDS Data API è abilitata.
- Il CloudTrail percorso ha la convalida dell'integrità dei file di registro abilitata.
- Il bucket Amazon S3 che CloudTrail percorri fornisce eventi per crittografare gli eventi utilizzando la crittografia SSE-S3 o SSE-KMS.
- Il bucket Amazon S3 a cui il CloudTrail percorso consegna l'evento ha la registrazione degli accessi al server abilitata.
- Il bucket Amazon S3 a cui distribuisci CloudTrail l'evento ha una configurazione del ciclo di vita che conserva i dati del CloudTrail percorso per almeno 18 mesi.

- Il bucket Amazon S3 a cui il CloudTrail percorso consegna l'evento ha Object Ownership impostato su Bucket owner applicato.
- Il bucket Amazon S3 a cui il CloudTrail percorso fornisce l'evento è accessibile da Accelerate.

Rivedi e aggiorna la policy sui bucket di Amazon S3 per la destinazione di consegna dei tuoi eventi CloudTrail

Durante l'onboarding, collabori con il tuo Cloud Architect (CA) per aggiungere dichiarazioni sulle policy relative ai bucket di Amazon S3 alla CloudTrail destinazione di distribuzione degli eventi. Per consentire ai tuoi utenti di richiedere le modifiche nel bucket Amazon S3 di destinazione di distribuzione CloudTrail degli eventi dal tuo account Accelerate, puoi implementare un ruolo IAM denominato in modo uniforme in ogni account dell'organizzazione gestito da Accelerate e aggiungerlo all'elenco in `aws:PrincipalArn` tutte le dichiarazioni politiche sui bucket di Amazon S3. Con questa configurazione, gli utenti possono interrogare e analizzare gli eventi del percorso CloudTrail organizzativo del tuo account in Accelerate utilizzando Athena. Per ulteriori informazioni su come aggiornare una policy sui bucket di Amazon S3, consulta Aggiungere una policy bucket utilizzando la console Amazon S3 nella Guida per l'utente di Amazon Simple Storage Service.

Important

L'aggiornamento della policy sui bucket Amazon S3 è necessario solo quando Accelerate si integra con un CloudTrail trail che fornisce eventi a un bucket S3 centralizzato. Accelerate non supporta l'integrazione con un CloudTrail trail che effettua consegne a un bucket centralizzato ma non dispone di account sotto un'organizzazione. AWS

Note

Prima di aggiornare la tua policy sui bucket di Amazon S3, sostituisci *red* i campi con i valori applicabili:

- *amzn-s3-demo-bucket*con il nome del bucket Amazon S3 che contiene gli eventi trail dei tuoi account.
- *your-organization-id*con l'ID dell' AWS organizzazione di cui i tuoi account sono membri.

- *your-optional-s3-log-delievery-prefix*con il CloudTrail prefisso di consegna del bucket Amazon S3 del percorso. Ad esempiomy-bucket-prefix, che potresti aver impostato al momento della creazione del percorso. CloudTrail

  Se non hai configurato un prefisso Amazon S3 bucket Delivery per il tuo percorso, rimuovi "*your-optional-s3-log-delievery-prefix*" e la barra progressiva () / dalle seguenti istruzioni sulla politica relativa ai bucket di Amazon S3.

Le seguenti tre dichiarazioni sulla politica dei bucket Amazon S3 concedono ad Accelerate l'accesso per recuperare le configurazioni ed eseguire query AWS Athena per analizzare gli eventi nel bucket Amazon S3 di destinazione di distribuzione degli eventi dal CloudTrail tuo account Accelerate.

```
{
    "Sid": "DONOTDELETE-AMS-ALLOWBUCKETCONFIGAUDIT",
    "Effect": "Allow",
    "Principal": {
        "AWS": "*"
    },
    "Action": [
        "s3:GetBucketLogging",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetEncryptionConfiguration"
    ],
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
    "Condition": {
        "StringEquals": {
            "aws:PrincipalOrgID": "your-organization-id"
        },
        "ArnLike": {
            "aws:PrincipalArn": [
                "arn:aws:iam::*:role/ams-access-*"
            ]
        }
    }
},
{
    "Sid": "DONOTDELETE-AMS-ALLOWLISTBUCKET",
    "Effect": "Allow",
    "Principal": {
        "AWS": "*"
```

```
    },
    "Action": "s3:ListBucket",
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
    "Condition": {
        "ForAnyValue:StringEquals": {
            "aws:CalledVia": "athena.amazonaws.com"
        },
        "StringLike": {
            "s3:prefix": "your-optional-s3-log-delievery-prefix/AWSLogs/*"
        },
        "StringEquals": {
            "aws:PrincipalOrgID": "your-organization-id"
        },
        "ArnLike": {
            "aws:PrincipalArn": [
                "arn:aws:iam::*:role/ams-access-*"
            ]
        }
    }
},
{
    "Sid": "DONOTDELETE-AMS-ALLOWGETOBJECT",
    "Effect": "Allow",
    "Principal": {
        "AWS": "*"
    },
    "Action": "s3:GetObject",
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/your-optional-s3-log-delievery-
prefix/AWSLogs/*",
    "Condition": {
        "ForAnyValue:StringEquals": {
            "aws:CalledVia": "athena.amazonaws.com"
        },
        "StringEquals": {
            "aws:PrincipalOrgID": "your-organization-id"
        },
        "ArnLike": {
            "aws:PrincipalArn": [
                "arn:aws:iam::*:role/ams-access-*"
            ]
        }
    }
}
```

Rivedi e aggiorna la politica chiave per la destinazione di distribuzione degli eventi AWS KMS CloudTrail

Durante l'onboarding, collabori con il tuo Cloud Architect (CA) per aggiornare la policy AWS KMS chiave utilizzata per crittografare gli eventi CloudTrail trail distribuiti al tuo bucket Amazon S3. Assicurati di aggiungere le dichiarazioni politiche AWS KMS chiave di riferimento alla chiave esistente. AWS KMS Ciò configura Accelerate per l'integrazione con il bucket Amazon S3 di distribuzione di eventi CloudTrail trail esistente e decrittografa gli eventi. Per consentire ai tuoi utenti di richiedere le modifiche nel bucket Amazon S3 di destinazione di distribuzione CloudTrail degli eventi dal tuo account Accelerate, puoi implementare un ruolo IAM denominato in modo uniforme in ogni account dell'organizzazione gestito da Accelerate e aggiungerlo all'elenco «aws:». PrincipalArn Con questa configurazione, gli utenti possono interrogare gli eventi.

Esistono diversi scenari AWS KMS chiave di aggiornamento delle politiche da prendere in considerazione. Potresti avere solo una AWS KMS chiave configurata per il tuo CloudTrail percorso per crittografare tutti gli eventi e non avere una AWS KMS chiave che crittografa gli oggetti nel tuo bucket Amazon S3. In alternativa, potresti avere una AWS KMS chiave che crittografa gli eventi forniti da CloudTrail e un'altra AWS KMS chiave che crittografa tutti gli oggetti archiviati nel tuo bucket Amazon S3. Se disponi di due AWS KMS chiavi, aggiorni la policy delle chiavi per ciascuna AWS KMS chiave per concedere ad Accelerate l'accesso ai tuoi eventi. CloudTrail Assicurati di modificare la dichiarazione politica AWS KMS chiave di riferimento con la politica AWS KMS chiave esistente prima di aggiornare la politica. Per ulteriori informazioni su come aggiornare una politica AWS KMS chiave, consulta Modifica di una politica chiave nella Guida per l'AWS Key Management Service utente.

> **Important**
>
> È necessario aggiornare la politica AWS KMS chiave solo quando Accelerate si integra con un CloudTrail percorso con la crittografia SSE-KMS dei file di registro abilitata.

> **Note**
>
> Prima di applicare questa dichiarazione sulla politica AWS KMS chiave alla AWS KMS chiave utilizzata per crittografare AWS CloudTrail gli eventi distribuiti al bucket Amazon S3, sostituisci i *red* seguenti campi con i valori applicabili:

- *YOUR-ORGANIZATION-ID*con l'ID dell' AWS organizzazione di cui i tuoi account sono membri.

Questa dichiarazione politica AWS KMS chiave garantisce ad Accelerate l'accesso agli eventi di decrittografia e query trail distribuiti al bucket Amazon S3 da ogni account dell'organizzazione con accesso limitato ad Athena, utilizzata da Accelerate per interrogare e analizzare gli eventi. CloudTrail .

```
{
    "Sid": "DONOTDELETE-AMS-ALLOWTRAILOBJECTDECRYPTION",
    "Effect": "Allow",
    "Principal": {
        "AWS": "*"
    },
    "Action": [
        "kms:Decrypt",
        "kms:DescribeKey"
    ],
    "Resource": "*",
    "Condition": {
        "ForAnyValue:StringEquals": {
            "aws:CalledVia": "athena.amazonaws.com"
        },
        "StringEquals": {
            "aws:PrincipalOrgID": "YOUR-ORGANIZATION-ID"
        },
        "ArnLike": {
            "aws:PrincipalArn": [
                "arn:aws:iam::*:role/ams-access-*"
            ]
        }
    }
}
```

Il modello per creare ruoli AMS

Il seguente ruolo AMS concede le autorizzazioni al tuo architetto cloud AMS (CA). Il seguente file zip contiene il codice e il CloudFormation modello Terraform che semplificano la creazione del ruolo IAM,

della politica di autorizzazione e della politica di fiducia. Per ulteriori informazioni, rivolgetevi al vostro CA.

Nome ruolo	Richiesto da	Modelli di esempio
`aws_managedservices_onboarding_role`	Personale AMS solo durante l'onboarding	onboarding_role_minimal.zip

> **Note**
>
> Dopo aver selezionato e scaricato un modello di esempio (uno per ruolo), lo caricherai come definizioni di CloudFormation stack inCrea `aws_managedservices_onboarding_role` con CloudFormation for Accelerate.

Crea **`aws_managedservices_onboarding_role`** con CloudFormation for Accelerate

Puoi creare il AWS Identity and Access Management ruoloaws_managedservices_onboarding_role, con CloudFormation from Console di gestione AWS. In alternativa, puoi utilizzare i comandi di AWS CloudShell per distribuire il ruolo.

Usa il Console di gestione AWS

> **Note**
>
> Prima di iniziare, tieni pronto per il caricamento un file JSON o YAML per ogni ruolo. Per ulteriori informazioni, consulta Il modello per creare ruoli AMS.

Per creare il ruolo da Console di gestione AWS, completa i passaggi seguenti:

1. Accedi Console di gestione AWS e apri la CloudFormation console all'indirizzo https://console.aws.amazon.com/cloudformazione.

2. Scegli Crea stack > Con nuove risorse (standard). Viene visualizzata la pagina seguente.

3. Scegli Carica un file modello, carica il file JSON o YAML del ruolo IAM, quindi scegli Avanti. Viene visualizzata la pagina seguente.

4. Inserisci il nome dello stack "**`ams-onboarding-role`**" nel campo Nome pila. Inserisci un DateOfExpiryutilizzando il formato «YYYY-MM-DDT 00:00:00 Z» (si consigliano 30 giorni dalla data corrente). Continua a scorrere verso il basso e seleziona Avanti fino a raggiungere questa pagina:

5. Assicurati che la casella di controllo sia selezionata, quindi seleziona Crea pila.
6. Assicurati che lo stack sia stato creato correttamente.

Usa i comandi di AWS CloudShell

Per distribuire il ruolo `aws_managedservices_onboarding_role` IAM, esegui il seguente comando in AWS CloudShell:

AWS CLI

```
curl -s "https://docs.aws.amazon.com/en_us/managedservices/latest/accelerate-guide/
samples/onboarding_role_minimal.zip" -o "onboarding_role_minimal.zip"
unzip -q -o onboarding_role_minimal.zip
aws cloudformation create-stack \
    --stack-name "aws-managedservices-onboarding-role" \
    --capabilities CAPABILITY_NAMED_IAM \
    --template-body file://onboarding_role_minimal.json \
    --parameters ParameterKey=DateOfExpiry,ParameterValue="`date -d '+30 days' -u '+
%Y-%m-%dT%H:%M:%SZ'`"
```

AWS Tools for PowerShell

```
Invoke-WebRequest -Uri 'https://docs.aws.amazon.com/en_us/managedservices/
latest/accelerate-guide/samples/onboarding_role_minimal.zip' -OutFile
 'onboarding_role_minimal.zip'
Expand-Archive -Path 'onboarding_role_minimal.zip' -DestinationPath . -Force
New-CFNStack `
```

```
    -StackName 'aws-managedservices-onboarding-role' `
    -Capability CAPABILITY_NAMED_IAM `
    -TemplateBody (Get-Content 'onboarding_role_minimal.json' -Raw) `
    -Parameter @{ParameterKey = "DateOfExpiry"; ParameterValue = (Get-
Date).AddDays(30).ToString('yyyy-MM-ddTHH:mm:ssZ')}
```

Dopo aver creato il ruolo, collabora con il tuo Cloud Architect (CA) per completare il Fase 2: Risorse di gestione dell'onboarding in Accelerate processo. Dopo che AMS ti ha informato che il tuo account è attivo, sei pronto per l'onboarding delle tue istanze.

Fase 3. Integrazione delle funzionalità AMS con policy predefinite

In questa fase, integri le funzionalità AMS con policy predefinite. Queste includono l'aggiunta di EC2 istanze Amazon e la configurazione di monitoraggio, backup, AWS Config correzione e patch (se applicabile, AMS Patch Orchestrator è un componente aggiuntivo che devi richiedere specificamente) in base alle tue preferenze. Puoi farlo da solo o richiedere che AMS integri le funzionalità in base ai tuoi input. Per richiedere assistenza ad AMS, crea una richiesta di assistenza e fornisci tutti gli input necessari per completare l'attività. Ricorda che le richieste di assistenza non vengono risolte immediatamente.

> **Note**
>
> Sebbene un account possa utilizzare criteri predefiniti per il backup, le patch o il monitoraggio, è necessario etichettare le risorse affinché la politica appropriata sia efficace.

Argomenti

- (Facoltativo) Modello Quick Start in Accelerate
- Onboarding Accelera il monitoraggio
- EC2 Istanze di onboarding per accelerare
- Inserimento in Accelerate AWS Backup
- Applicazione delle patch di onboarding in Accelerate
- Esamina i report di non conformità in Accelerate

(Facoltativo) Modello Quick Start in Accelerate

Il modello Quick Start automatizza l'implementazione e la configurazione di AMS Resource Tagger negli account abilitati ad AWS Accelerate. Questo modello consente di risparmiare tempo e fatica rispetto alla configurazione manuale. Utilizza questo modello così com'è per definire le nozioni di base di monitoraggio, applicazione di patch e backup in un unico account. Oppure, usalo StackSet per applicare le impostazioni tra le Organizations Units per standardizzare le impostazioni per più account.

Puoi anche usarlo come punto di partenza per creare il tuo profilo AMS Resource Tagger personalizzato e utilizzare frammenti della documentazione per creare definizioni più complesse per l'etichettatura.

Funzionalità del modello Quick Start

Il modello Quick Start completa le seguenti attività:

- Crea e distribuisce una versione di configurazione per AMS Resource Tagger.
- Applica tag alle EC2 istanze Amazon che consentono la gestione AMS e la creazione di risorse di monitoraggio.
- (Facoltativo) Applica tag alle EC2 istanze gestite che consentono di applicare le patch secondo la pianificazione desiderata e crea una finestra di manutenzione delle patch per facilitare l'applicazione delle patch.

  > **Warning**
  >
  > Per impostazione predefinita, le istanze vengono riavviate e le istanze interrotte vengono avviate automaticamente per l'installazione delle patch.

- (Facoltativo) Applica tag alle EC2 istanze gestite che ne consentono il backup come definito nel piano di backup AMS predefinito.
- (Facoltativo) Applica tag alle risorse gestite di Amazon Relational Database Service (Amazon RDS) che ne consentono il backup secondo il piano di backup Enhanced. Un piano di backup consente inoltre il ripristino in tempo reale (PITR) per Amazon RDS. Se il backup automatico di Amazon RDS non è abilitato, il database si riavvia in prossimità della finestra di backup successiva.

Sostituzioni ed esclusioni del modello Quick Start

Dopo aver utilizzato questo modello per creare uno stack Quick Start, utilizza i seguenti passaggi per escludere istanze specifiche da Gestione/Monitoraggio, Patching o Backup:

- Gestione e monitoraggio: per escludere un' EC2 istanza dalla gestione e dal monitoraggio da parte di AMS, aggiungi questo tag all'istanza:. `ExcludeFromAMSQuickStartMonitoring=true`
- Applicazione di patch: EC2 le istanze che fanno parte di un gruppo Auto Scaling, Amazon Elastic Container Service o un cluster Amazon Elastic Kubernetes Service sono escluse dall'applicazione delle patch tramite questo modello Quick Start.

  Per disabilitare la creazione di una finestra di patching e l'etichettatura delle istanze relativa alla patch, imposta il parametro stack su. EC2 CloudFormation `EnablePatching=false`

  Per escludere un' EC2 istanza dalla finestra di patching di Quick Start quando`EnablePatching=true`, aggiungi questo tag all'istanza:. `ExcludeFromAMSQuickStartPatching=true`
- Backup: EC2 le istanze che fanno parte di un gruppo di Auto Scaling, di un cluster ECS o EKS sono escluse dal Backup tramite questo modello Quick Start.

  Per escludere un' EC2 istanza dall'obiettivo del piano di Backup AMS predefinito, quando`EnableBackup=true`, aggiungi questo tag a quell'istanza:`ExcludeFromAMSQuickStartBackup=true`.

> **Tip**
>
> Puoi taggare EC2 le istanze in blocco. Usa Tag Editor per selezionare in blocco e contrassegnare le risorse in un unico passaggio del. Console di gestione AWS

Parametri del modello Quick Start

Questo modello Quick Start configura Resource Tagger per aggiungere il tag `ams:rt:ams-managed=true` a tutte le EC2 istanze dell'account, escluse le istanze a cui aggiungi il tag. `ExcludeFromAMSQuickStartMonitoring=true` Utilizza i seguenti parametri per controllare le parti opzionali di questo stack in base alle tue esigenze:

Parametro CFN	Valore	Effetto
EnableBackup	'true' (impostazione predefinita)	Tutte le EC2 istanze gestite da AMS (`ams:rt:ams-managed=true`) sono contrassegnate `ams:rt:backup-orchestrator=true` per il backup ogni giorno alle 4:00 UTC secondo il piano di backup AMS predefinito. Per tutte le istanze e i cluster RDS, il modello applica il `ams:rt:backup-orchestrator-enhanced=true` «backup continuo» con conservazione massima (31 giorni) come previsto dal piano di backup Enhanced. Se ciò modifica il periodo di conservazione PITR, il database potrebbe essere riavviato in alcuni casi, ad esempio se ci sono altri aggiornamenti di configurazione in sospeso.
	'falso'	Nessuna istanza è destinata al backup con questo modello di avvio rapido.
EnablePatching	'false' (impostazione predefinita)	Nessuna istanza è destinata all'applicazione di patch da questo modello Quick Start.
	'vero'	Tutte le istanze gestite da AMS (`ams:rt:ams-managed=true`) sono contrassegnate `ams:rt:Patch Group=AMSQuickStartPatchWindow` e viene creata

Parametro CFN	Valore	Effetto
		una risorsa di base della finestra di manutenzione SSM per facilitare l'applicazione delle patch in base alla pianificazione definita in. `CronExpression` Per applicare il `ams:rt:PatchGroup` tag all' EC2 istanza, è necessario disattivare l'accesso ai tag nei metadati dell'istanza per quell'istanza.
CronExpression	-	Il valore predefinito di `cron(0 30 19 ? * SAT#2 *)` imposta il secondo sabato del mese alle 19:30 in base al `Timezone` parametro. Usa la sintassi cron.
Fuso orario	-	Le istanze di Target vengono patchate in base a. `CronExpression` Usa il formato IANA.

Scarica il modello Quick Start

Scarica il file AMSQuick Start.zip.

In alternativa, esegui il comando seguente AWS CloudShellper distribuire: `AMSQuickStart.yaml`

AWS Command Line Interface

```
curl -s "https://docs.aws.amazon.com/en_us/managedservices/latest/accelerate-guide/
samples/AMSQuickStart.zip" -o "AMSQuickStart.zip"
unzip -q -o AMSQuickStart.zip
for region in region1 region2 ;
do
aws cloudformation create-stack \
    --region $region \
    --stack-name "AMSQuickStart" \
```

```
    --template-body file://AMSQuickStart.yaml \
    --parameters \
        ParameterKey=EnableBackup,ParameterValue="true" \
        ParameterKey=EnablePatching,ParameterValue="false" \
        ParameterKey=Timezone,ParameterValue="US/Eastern" \
        ParameterKey=CronExpression,ParameterValue="cron(0 30 19 ? * SAT#2 *)" \
;
done
```

AWS Tools for PowerShell

```
Invoke-WebRequest -Uri 'https://docs.aws.amazon.com/en_us/managedservices/latest/
accelerate-guide/samples/AMSQuickStart.zip' -OutFile 'AMSQuickStart.zip'
Expand-Archive -Path 'AMSQuickStart.zip' -DestinationPath . -Force
@('region1', 'region2') | `
ForEach-Object { `
New-CFNStack `
    -Region $_ `
    -StackName 'AMSQuickStart' `
    -TemplateBody (Get-Content 'AMSQuickStart.yaml' -Raw) `
    -Parameter @(
        @{ParameterKey = "EnableBackup"; ParameterValue = "true"},
        @{ParameterKey = "EnablePatching"; ParameterValue = "false"},
        @{ParameterKey = "Timezone"; ParameterValue = "US/Eastern"},
        @{ParameterKey = "CronExpression"; ParameterValue = "cron(0 30 19 ? * SAT#2
 *)"}
    )
}
```

Per una descrizione di ogni parametro, vedere la sezione precedente,. Parametri del modello Quick Start

Onboarding Accelera il monitoraggio

Il monitoraggio è abilitato per impostazione predefinita per tutte le nuove risorse ad eccezione delle istanze Amazon EC2. Puoi iniziare a monitorare le tue istanze Amazon EC2 etichettando le tue istanze.

Per quanto riguarda il monitoraggio integrato, assicurati innanzitutto che la configurazione monitori le risorse che desideri che AMS monitori e ignori le risorse che desideri vengano ignorate.

Puoi utilizzare le seguenti CloudWatch dashboard per scoprire quante delle tue risorse sono prese di mira dal monitoraggio e dall'etichettatura di AMS e quante no. Nel tuo account, accedi alla console delle CloudWatch dashboard e seleziona una delle seguenti opzioni:

- Pannello di controllo AMS-Alarm-Manager-Reporting
- Pannello di controllo AMS-Resource-Tagger-Reporting

Per una descrizione completa delle metriche del dashboard, consulta:

- Visualizzazione del numero di risorse gestite da Resource Tagger

Risorse di onboarding da monitorare in Accelerate

Per ignorare il comportamento predefinito, ad esempio per disabilitare il monitoraggio predefinito per le risorse non EC2, è necessario rimuovere i tag di tali risorse utilizzando un profilo di configurazione personalizzato. Per ulteriori informazioni sull'etichettatura per il monitoraggio, consulta. Monitoraggio in Accelere

Il monitoraggio è disabilitato per le istanze EC2 fino all'onboarding delle istanze, il che include l'etichettatura delle istanze utilizzando un profilo di configurazione personalizzato. La sezione successiva descrive l'onboarding delle istanze EC2.

Creazione di un profilo di configurazione di monitoraggio in Accelerate

- Per informazioni sull'utilizzo della configurazione predefinita, vedereAccelera Alarm Manager.
- Per informazioni sull'utilizzo di una configurazione personalizzata, vedereModifica della configurazione predefinita di Accelerate alarm.

EC2 Istanze di onboarding per accelerare

EC2 l'onboarding delle istanze in AMS Accelerate avviene tramite un processo chiamato Automated Instance Configuration, che assicura che ogni istanza scriva i log corretti ed emetta le metriche corrette per consentire ad AMS di gestire correttamente l'istanza. Dovresti effettuare l'onboarding di tutte le tue EC2 istanze, a meno che tu non voglia espressamente che AMS ne ignori alcune. La configurazione automatizzata dell'istanza richiede che vengano soddisfatte condizioni specifiche che consentano ad AMS di configurare l'istanza (per i dettagli, vederePrerequisiti per la configurazione automatica delle istanze in Accelerate). La condizione più importante è che l' AWS Systems Manager

agente (agente SSM) sia installato su ogni EC2 istanza Amazon che desideri che AMS gestisca per te. Per ulteriori informazioni sull'agente SSM, consulta Working with SSM agent.

SSM preinstallato nella versione standard di Accelerate AMIs

L'agente SSM è già installato su AWS-provided AMIs per i seguenti sistemi operativi.

- Amazon Linux e Amazon Linux 2
- SUSE Linux Enterprise Server (SLES) 12 e 15
- Microsoft Windows Server 2019, 2016, 2012 R2, 2012
- Ubuntu Linux 18.04 e 20.04

Se stai usando uno di questi AWS forniti, vedi AMIs. Etichettatura delle istanze in Accelerate

Installazione manuale SSM di SSM in Accelerate

Per i seguenti sistemi operativi o quando si utilizza un'AMI personalizzata, è possibile installare manualmente l'agente SSM. In alternativa, puoi utilizzare la funzione di installazione automatica dell'agente AMS SSM. Per ulteriori informazioni sull'installazione automatica di SSM, consultaInstallazione automatica di SSM Agent. Per istruzioni sull'installazione manuale, seleziona il collegamento relativo al tuo sistema operativo:

- Installazione CentOS SSM
- Installazione di Oracle SSM
- Installazione di Red Hat SSM
- Installazione SSM di SUSE Linux Enterprise Server
- Installazione di Windows SSM

Etichettatura delle istanze in Accelerate

Dopo aver installato l'agente SSM, è necessario etichettare le istanze. Per informazioni, consulta Etichettatura in AMS Accelerate.

Configurazione automatica delle istanze in Accelerate

Una volta etichettata l'istanza, AMS esegue una configurazione automatizzata dell'istanza, che include:

- Registra i log e le metriche del sistema operativo
- Abilita l'accesso remoto per gli ingegneri AMS
- Esegui comandi remoti sull'istanza

Queste attività sono essenziali per i servizi di monitoraggio, patch e log di AMS e per consentire ad AMS di rispondere agli incidenti. Per i dettagli sulla configurazione della configurazione automatizzata delle istanze, consultaConfigurazione automatica delle istanze in AMS Accelerate.

Una volta completata la configurazione automatizzata dell'istanza, puoi:

- Crea incidenti e richieste di assistenza per EC2 istanze e sistemi operativi Amazon utilizzando la console Support Center. Per ulteriori informazioni, consulta Segnalazioni di incidenti, richieste di assistenza e domande di fatturazione in AMS Accelerate.
- Accedi e controlla i EC2 log di Amazon
- Ottieni report sulle patch

Inserimento in Accelerate AWS Backup

Per configurare i backup, è necessario creare policy di backup denominate piani di backup. Un piano di backup specifica le AWS risorse di cui eseguire il backup, la frequenza di backup e il periodo di conservazione dei backup. Si consiglia di valutare i requisiti di continuità, sicurezza e conformità dell'organizzazione per determinare i piani di backup necessari.

Attivazione

- Assicurati che AWS Backup sia abilitato per ogni account, regione e tipo di risorsa seguendo i passaggi riportati di seguito:

  Guida introduttiva 1: Service Opt-in.

  Facoltativamente, Guida introduttiva 2: Crea un backup su richiesta.

Scegli un piano di backup

- Per scegliere un piano di backup, consultaSeleziona un piano di backup AMS.

Aggiungere risorse

Per impostazione predefinita, le risorse non sono associate a un piano di backup. Devono essere aggiunte a un piano di backup.

- Per aggiungere risorse a un piano di backup, vedereEtichetta le tue risorse per applicare i piani di backup AMS.
- Per abilitare il backup su tutte le risorse utilizzando i tag, vedereGestione dei tag per i backup in Accelerate.

Applicazione delle patch di onboarding in Accelerate

È necessario configurare l'applicazione delle patch per garantire che il software sia conforme up-to-date e soddisfi le politiche di conformità.

AWS Backup prerequisito: per consentire la creazione di uno snapshot del volume root durante la finestra di manutenzione dell'applicazione delle patch, assicurati che AWS Backup sia abilitato per ogni account e regione per il tipo di risorsa Amazon EBS seguendo i passaggi riportati qui: Guida introduttiva 1: Service Opt-in. (Non è necessario continuare con Getting started 2: Crea un backup su richiesta).

Quando applicare le patch: l'applicazione delle patch avviene durante una finestra di manutenzione. È possibile pianificare le finestre di manutenzione in modo che le patch vengano applicate solo durante gli orari preimpostati.

Cosa patchare: devi associare le EC2 istanze Amazon che desideri patchare a una finestra di manutenzione. Per associare le istanze a una finestra di manutenzione, le EC2 istanze Amazon devono essere etichettate e la finestra di manutenzione deve avere tali tag come destinazione.

Quali patch installare: utilizzando le linee di base delle patch, si impostano regole per l'approvazione automatica di determinati tipi di patch, come il sistema operativo o le patch ad alta gravità. È inoltre possibile specificare eccezioni alle regole, ad esempio elenchi di patch che vengono sempre approvate o rifiutate.

Consulta Consigli per l'applicazione delle patch le indicazioni sulle politiche EC2 delle patch di Amazon.

- Per iniziare a configurare la gestione delle patch, consulta Comprendi la gestione delle patch in AMS Accelerate
- Per creare una configurazione di patch personalizzata, vederePatch di base personalizzate con AMS Accelerate.

Esamina i report di non conformità in Accelerate

AMS implementa AWS Config regole che aiutano a identificare le violazioni degli standard stabiliti dal Center for Internet Security (CIS), dal National Institute of Standards and Technology (NIST) Cloud Security Framework (CSF). Ti consigliamo di esaminare il rapporto di non conformità con il tuo team di consegna per dare priorità alle azioni correttive in modo che il tuo account sia conforme.

Fase 4. Personalizza le funzionalità in Accelerate

In questa fase, hai già integrato il monitoraggio, l'applicazione di patch e il backup con policy predefinite. Ora avete la possibilità di personalizzare le policy in base alle vostre esigenze.

Puoi scegliere di utilizzare le politiche predefinite per patch, backup o monitoraggio oppure scegliere una politica personalizzata in base alle tue esigenze. AMS utilizza i tag per associare le risorse alle politiche operative. AMS fornisce un Resource Tagger che consente di specificare le regole su come i tag vengono applicati alle AWS risorse in base al raggruppamento delle applicazioni o ad altre logiche di raggruppamento. Per ulteriori informazioni, vedere. Accelera Resource Tagger

La funzionalità di tag fornita dal cliente consente di aggiungere ed eliminare tag personalizzati alle risorse AMS. Per ulteriori informazioni, consulta Tag forniti dal cliente in Accelerate.

Argomenti

- Personalizza il monitoraggio in Accelerate
- Personalizza il backup in Accelerate
- Personalizza l'applicazione delle patch in Accelerate

Personalizza il monitoraggio in Accelerate

Per personalizzare il monitoraggio delle risorse cloud in base alle esigenze delle applicazioni:

1. Crea una politica di monitoraggio personalizzata. Per informazioni, consulta Modifica della configurazione predefinita di Accelerate alarm.
2. Applica una politica personalizzata alle risorse utilizzando i tag. Per informazioni, consultare Monitoraggio in Accelere.
3. Indirizza gli avvisi al proprietario della risorsa. Per informazioni, consulta Notifica di avviso basata su tag.

Puoi utilizzare le seguenti CloudWatch dashboard per scoprire quante delle tue risorse sono prese di mira dal monitoraggio e dall'etichettatura di AMS e quante no. Nel tuo account, accedi alla console delle CloudWatch dashboard e seleziona una delle seguenti opzioni:

- Pannello di controllo AMS-Alarm-Manager-Reporting
- Pannello di controllo AMS-Resource-Tagger-Reporting

Per una descrizione completa delle metriche del dashboard, consulta:

- Visualizzazione del numero di risorse gestite da Resource Tagger

Personalizza il backup in Accelerate

Non è possibile personalizzare i piani di backup predefiniti di AMS. Invece, crea un nuovo piano di backup in base alle esigenze dell'applicazione, quindi allega le risorse al piano personalizzato utilizzando i tag. Spetta a voi scegliere di quali risorse AMS deve eseguire il backup, con quale frequenza e per quale periodo di conservazione. Consigliamo di valutare i requisiti di continuità, sicurezza e conformità della vostra organizzazione per determinare i piani di backup necessari.

- Per creare un piano di backup, consulta Creazione di un piano di backup.
- Per assegnare risorse a un piano di backup, vedere Assegnazione di risorse a un piano di backup.

Personalizza l'applicazione delle patch in Accelerate

L'applicazione delle patch garantisce che il software sia conforme up-to-date e soddisfi le politiche di conformità.

Quando applicare le patch: l'applicazione delle patch avviene durante una finestra di manutenzione. È possibile pianificare le finestre di manutenzione in modo che le patch vengano applicate solo durante gli orari preimpostati.

Cosa patchare: devi associare le EC2 istanze Amazon che desideri patchare a una finestra di manutenzione. Per associare le istanze a una finestra di manutenzione, le EC2 istanze Amazon devono essere etichettate e la finestra di manutenzione deve avere tali tag come destinazione.

Quali patch installare: utilizzando le linee di base delle patch, si impostano regole per l'approvazione automatica di determinati tipi di patch, come il sistema operativo o le patch ad alta gravità. È inoltre

possibile specificare eccezioni alle regole, ad esempio elenchi di patch che vengono sempre approvate o rifiutate.

- Per consigli generali sull'applicazione delle patch, consulta. Consigli per l'applicazione delle patch
- Per creare finestre di manutenzione personalizzate, vedereCreare una finestra di manutenzione delle patch in AMS.
- Per creare linee base di patch personalizzate, vedere. Patch di base personalizzate con AMS Accelerate
- Per inoltrare gli avvisi di patch al proprietario della risorsa, vedere. Comprendi le notifiche e gli errori delle patch in AMS Accelerate

Uso delle console AMS

Le console AMS nella console di AWS gestione sono disponibili per interagire con AMS e utilizzare le risorse gestite da AMS Advanced e AMS Accelerate. Le console AMS generalmente si comportano come qualsiasi AWS console; tuttavia, poiché AMS è un'organizzazione privata, solo gli account abilitati per AMS possono accedere alla console. Una volta abilitato AMS nel tuo account, puoi accedere alla console cercando «Managed Services» nella barra di ricerca unificata.

> **Note**
>
> A seconda del ruolo dell'account, accedi alla console AMS Advanced o alla console AMS Accelerate.

Quando utilizzi le console AMS, tieni presente le seguenti avvertenze:

- La console AMS è specifica per ogni account. Pertanto, se utilizzi un account «Test» per la tua organizzazione, non potrai visualizzare le risorse nell'account «Prod» di quell'organizzazione. Allo stesso modo, devi avere un ruolo AMS Advanced per accedere alla console AMS Advanced.
- Le console AMS applicano una policy IAM al momento dell'autenticazione che determina a quale console puoi accedere e cosa puoi fare in quella sede. L'amministratore può applicare politiche aggiuntive alla politica AMS predefinita per limitare ciò che puoi vedere e fare nella console.

La console AMS Accelerate ha le seguenti funzionalità:

- Pagina di apertura: la pagina di apertura contiene riquadri informativi e link per facilitare l'accesso ai report agli incidenti, alle richieste di assistenza e ai report.
- Pagine di funzionalità, collegamenti nel riquadro di navigazione a sinistra:
  - Dashboard: fornisce una panoramica dello stato attuale del tuo account, tra cui:
    - Incidenti sulle tue risorse: un pulsante per aprire un caso di incidente in AWS Support Center, oltre a quanti casi di incidente sono in attesa di approvazione e richiedono la tua attenzione e quanti sono aperti
    - Stato di conformità: collegamenti a regole e risorse non conformi o conformi
    - Richieste di assistenza: un pulsante per aprire un caso di richiesta di assistenza in AWS Support Center, oltre a quante sono in attesa di approvazione e richiedono la tua attenzione e quante sono aperte
    - Sicurezza a livello di account: collegamenti ai dettagli sui risultati del rilevamento delle minacce in tempo reale e sui GuardDuty risultati di Macie sulla sicurezza e la privacy dei dati
    - Azioni rapide: apri le pagine di configurazione degli archivi di Backup o delle istanze di Patch
  - Rapporti: apre la pagina Report e i report predefiniti, Backup giornaliero e Patch giornalieri e Fatturazione mensile
  - Configurazione: assicurati che le tue risorse vengano gestite correttamente e in base alle tue specifiche.
    - Installa l'agente SSM: è richiesto l'agente SSM
    - Configura le regole di tagging: apre AMS Resource Tagger
    - Configura gli allarmi: apre la configurazione degli allarmi AMS CloudWatch
    - Configurazione della pianificazione delle patch: apre la console AWS Systems Manager
    - Configurazione delle linee di base delle patch: apre la console AWS Patch Manager
    - Configurazione dei piani di backup: apre la console AWS Backup
- Funzionalità in primo piano: informazioni sugli ultimi aggiornamenti della console
- Documentazione: pagina iniziale della documentazione di AWS Managed Services

Modelli AMS

Un modello AWS Managed Services (AMS) è una soluzione generalizzata che risolve una famiglia di casi d'uso nell'ambiente gestito AMS.

Mentre operi sulla piattaforma AMS, gli architetti cloud AMS (CAs) collaborano con te per soddisfare i tuoi requisiti aziendali e operativi. Sebbene i clienti AMS operino in modo unico, notiamo che i clienti hanno casi d'uso simili. In questi casi, CAs crea modelli di soluzione generali, o «modelli», da utilizzare in più ambienti di clienti con uno sforzo minimo di configurazione e implementazione.

I modelli AMS sono creati per aiutare a fornire funzionalità ai clienti AMS e di solito vengono creati dall'account CA del cliente che li richiede.

Come funzionano i pattern AMS

Per richiedere maggiori dettagli su ogni pattern, compresi i modelli di cloudformation necessari per poter implementare il pattern, invia una richiesta di servizio AMS con l'oggetto «Richiesta di ulteriori dettagli sul pattern***Pattern_Name***» (sostituisci il modello che desideri) e aggiungi il tuo architetto cloud AMS (CA) all'opzione Contatti aggiuntivi.

I pattern AMS sono classificati in due (2) categorie:

- Uso generale: i pattern sono considerati stabili in quanto sono stati implementati e utilizzati da più clienti AMS
- Modalità di anteprima: AMS consiglia di implementare i modelli della modalità di anteprima negli ambienti non di produzione per la convalida e di contattare Cloud Architect per discutere del caso d'uso prima dell'implementazione.

> **Important**
>
> I modelli AMS non rispettano i Service Level Agreements () e gli Obiettivi di servizio () predefiniti degli AMS Service Level Agreements (SLAs) e degli Obiettivi di servizio (). SLOs Support e aggiornamenti del pattern vengono eseguiti con la massima diligenza.
> Questo AWS contenuto viene fornito in base ai termini del Contratto con il AWS cliente o altro accordo scritto tra il cliente e Amazon Web Services, Inc. o Amazon Web Services EMEA SARL («AWS Europe») o entrambi.
> Il materiale contenuto in questo software viene fornito all'utente «così com'è» e senza garanzie di alcun tipo, esplicite, implicite o di altro tipo, inclusa, a titolo esemplificativo, qualsiasi garanzia di idoneità per uno scopo particolare.

Modelli AMS

Modelli AMS.

Modelli AMS

Nome	Panoramica	Vantaggi	Categoria
Personalizza le notifiche di CloudWatch allarme	Personalizza le notifiche di CloudWatch allarme per includere informazioni dai tag delle istanze come il nome dell'istanza, l'ID dell'applicazione e così via.	L'aggiunta di informazioni contestuali alle notifiche di allarme le renderà più significative e fornirà informazioni utilizzabili.	Monitoraggio
Rapporti sull'utilizzo del disco	Il modello Disk Usage Reporting raccoglie lo spazio di consumo dei volumi su più account di app e presenta i risultati sotto forma di report centralizzato in Amazon S3 con funzionalità di interrogazione delle tabelle Athena.	Fornisci informazioni sull'utilizzo effettivo dei volumi degli account per determinare le opportunità di risparmio sui costi.	Ottimizzazione dei costi
Prowler Stack	Esegue controlli Prowler sugli account che utilizzano Amazon, EC2 dove non CloudShell possono essere utilizzati.	Aiutaci a sbloccare Accelerate onboarding (Prowler) nei casi in cui non CloudShell può essere utilizzato a causa di autorizzazioni o problemi di timeout senza alcun impatto sul	Sicurezza

Nome	Panoramica	Vantaggi	Categoria
		loro attuale livello di sicurezza.	
Replica AMS Amazon S3 con chiavi oggetto personalizzate	Crea copie degli oggetti Amazon S3 e conserva tutti i metadati e le chiavi degli oggetti (cartelle). Rimuove parte delle chiavi dell'oggetto di origine o crea chiavi dell'oggetto di destinazione personalizzate durante la replica.	Personalizza le chiavi degli oggetti (cartelle) durante la replica di Amazon S3 senza richiedere script aggiuntivi per spostare gli oggetti nelle cartelle richieste.	Affidabilità
Eliminazione di snapshot Amazon EBS	Automazione basata su Lambda ed CloudWatch Events per automatizzare l'eliminazione degli snapshot di Amazon EBS acquisiti all'esterno, in base alla conservazione. AWS Backup	Aiuta a eliminare le singole istantanee scattate al di fuori dell' AWS Backup orchestrator, risparmiando costi aggiuntivi nel tempo.	Ottimizzazione dei costi

Nome	Panoramica	Vantaggi	Categoria
Rotazione dei segreti di AMS Amazon RDS	Utilizzando un CloudFormation modello, distribuisci automaticamente tutte le risorse richieste (funzione Lambda, gruppi di sicurezza , interfacce di rete elastiche ENIs o) necessarie per la rotazione dei segreti per i database Amazon RDS supportati, Redshift e DocumentDB.	Automatizza la rotazione dei segreti del database e fornisci un meccanism o di notifica quando si verifica un errore di rotazione.	Sicurezza
Rotazione automatica delle chiavi	Ruota automatic amente le chiavi di accesso e segrete per gli utenti IAM in base a CloudWatch Events e Lambda.	Rotazione più semplice delle chiavi di accesso e segrete per gli utenti IAM.	Sicurezza

Nome	Panoramica	Vantaggi	Categoria
Tagger per snapshot di volume Amazon EBS	Etichetta tutti i volumi e gli snapshot di Amazon EBS utilizzando i tag nelle istanze Amazon EC2 .	Aiuta a classificare e tenere traccia dei costi con informazioni aziendali significative e pertinenti, che semplificano la convalida di dove vengono spesi i soldi e consenti l'uso dell'automazione per volumi e istantanee con tag. Best practice altamente consigliata dal pilastro dell'ottimizzazione dei costi AWS .	Etichettatura (ottimizzazione dei costi, sicurezza, gestione degli incidenti e automazione)

Configurazione automatica delle istanze in AMS Accelerate

AMS Accelerate fornisce un servizio di configurazione automatica delle istanze. Questo servizio garantisce che un'istanza emetta i log e le metriche corretti per consentire ad AMS di gestire correttamente l'istanza. La configurazione automatizzata dell'istanza ha i propri prerequisiti e passaggi per l'onboarding, descritti più avanti in questa sezione.

Argomenti

- Come funziona la configurazione automatica delle istanze in Accelerate
- Installazione automatica di SSM Agent
- Modifiche automatiche alla configurazione delle ist

Come funziona la configurazione automatica delle istanze in Accelerate

La configurazione automatizzata delle istanze consente ad AMS Accelerate di eseguire determinate configurazioni su base giornaliera su istanze indicate aggiungendo agenti e tag particolari.

Prerequisiti per la configurazione automatica delle istanze in Accelerate

Queste condizioni devono essere soddisfatte per consentire ad AMS Accelerate di eseguire le azioni automatizzate descritte in precedenza sulle istanze gestite.

L'agente SSM è installato

La configurazione automatizzata dell'istanza di AMS Accelerate richiede l'installazione dell'agente AWS Systems Manager SSM.

Per informazioni sull'utilizzo della funzionalità di installazione automatica dell'agente AMS SSM, vedereInstallazione automatica di SSM Agent.

Per informazioni sull'installazione manuale dell'agente SSM, consulta quanto segue:

- Linux: installa manualmente SSM Agent su EC2 istanze Amazon per Linux - AWS Systems Manager
- Windows: installa manualmente SSM Agent su EC2 istanze Amazon per Windows Server - AWS Systems Manager

L'agente SSM è nello stato gestito

La configurazione automatizzata delle istanze di AMS Accelerate richiede un agente SSM operativo. L'agente SSM deve essere installato e l' EC2 istanza Amazon deve trovarsi nello stato gestito. Per ulteriori informazioni, consulta la AWS documentazione, Working with SSM Agent.

Configurazione automatica delle istanze

Supponendo che i prerequisiti siano stati soddisfatti, l'aggiunta di un tag di EC2 istanza Amazon specifico avvia automaticamente la configurazione automatizzata dell'istanza AMS Accelerate. Utilizza uno dei seguenti metodi per aggiungere questo tag:

1. (Consigliato vivamente) Usa l'AMS Accelerate Resource Tagger

   Per configurare la logica di tagging per il tuo account, consulta. Come funziona il tagging Una volta completata l'etichettatura, i tag e la configurazione automatica dell'istanza vengono gestiti automaticamente.
2. Aggiungere manualmente i tag

   Aggiungi manualmente il seguente tag alle EC2 istanze Amazon:

Chiave: ams:rt:ams-managed, Valore: true.

> **Note**
>
> Il servizio di configurazione dell'istanza tenta di applicare le configurazioni AMS richieste una volta che il tag ams:rt:ams-managed viene applicato all'istanza. Il servizio afferma le configurazioni richieste da AMS ogni volta che viene avviata un'istanza e quando viene effettuato un controllo giornaliero della configurazione di AMS.

Installazione automatica di SSM Agent

> **Important**
>
> L'installazione automatica di SSM Agent non supporta la regione Asia Pacifico (Malesia).

Per fare in modo che AMS gestisca le tue istanze Amazon Elastic Compute Cloud (Amazon EC2), devi AWS Systems Manager installare SSM Agent su ogni istanza. Se sulle istanze non è installato SSM Agent, puoi utilizzare la funzionalità di installazione automatica di AMS SSM Agent.

> **Note**
>
> - Se il tuo account viene registrato su AMS Accelerate dopo il 6/03/2024, questa funzionalità è abilitata per impostazione predefinita. Per disattivare questa funzionalità, contatta il tuo CA o il CSDM.
> - Per attivare questa funzionalità negli account registrati prima del 6/03/2024, contatta la tua CA o il CSDM.
> - Questa funzionalità è disponibile solo per le istanze EC2 che non fanno parte di un gruppo Auto Scaling e che eseguono sistemi operativi Linux supportati da AMS.

Prerequisiti per l'utilizzo di SSM Agent

- Assicurati che il profilo di istanza associato alle istanze di destinazione abbia una delle seguenti politiche (o autorizzazioni equivalenti a quelle consentite in esse):

  - Amazon SSMManaged EC2 InstanceDefaultPolicy
  - Amazon SSMManaged InstanceCore
- Assicurati che non esista una Service Control Policy al AWS Organizations livello che neghi esplicitamente le autorizzazioni elencate nelle politiche precedenti.

  Per ulteriori informazioni, consulta la pagina Configurazione delle autorizzazioni dell'istanza richieste per Systems Manager.
- Per bloccare il traffico in uscita, assicurati che i seguenti endpoint di interfaccia siano abilitati sul VPC in cui risiedono le istanze di destinazione (sostituisci «regione» nell'URL in modo appropriato):
  - ssm.<regione>.amazonaws.com
  - ssmmessages.<regione>.amazonaws.com
  - messaggi ec2. <region>.amazonaws.com

  Per ulteriori informazioni, consulta Migliora la sicurezza delle istanze EC2 utilizzando gli endpoint VPC per Systems Manager.

Per suggerimenti generali sull'attivazione o la risoluzione dei problemi relativi alla disponibilità dei nodi gestiti, consulta Soluzione 2: verifica che sia stato specificato un profilo di istanza IAM per l'istanza (solo istanze EC2).

> **Note**
>
> AMS arresta e avvia ogni istanza come parte del processo di installazione automatica. Quando un'istanza viene interrotta, i dati archiviati nei volumi di archiviazione delle istanze e i dati archiviati nella RAM vengono persi. Per ulteriori informazioni, consulta Cosa succede quando si interrompe un'istanza.

Richiedi l'installazione automatica di SSM Agent sulle tue istanze

Se i tuoi account sono registrati su AMS Accelerate Patch Add-On, configura una finestra di manutenzione delle patch (MW) per le istanze. È necessario un agente SSM funzionante per completare il processo di patch. Se l'agente SSM non è presente su un'istanza, AMS tenta di installarlo automaticamente durante la finestra di manutenzione della patch.

> **Note**
>
> AMS arresta e avvia ogni istanza come parte del processo di installazione automatica. Quando un'istanza viene interrotta, i dati archiviati nei volumi di archiviazione delle istanze e i dati archiviati nella RAM vengono persi. Per ulteriori informazioni, consulta Cosa succede quando si interrompe un'istanza.

Come funziona l'installazione automatica di SSM Agent

AMS utilizza i dati utente EC2 per eseguire lo script di installazione sulle tue istanze. Per aggiungere lo script dei dati utente ed eseguirlo sulle istanze, AMS deve arrestare e avviare ogni istanza.

Se l'istanza ha già uno script di dati utente esistente, AMS completa i seguenti passaggi durante il processo di installazione automatica:

1. Crea un backup dello script di dati utente esistente.
2. Sostituisce lo script dei dati utente esistente con lo script di installazione di SSM Agent.
3. Riavvia l'istanza per installare SSM Agent.
4. Arresta l'istanza e ripristina lo script originale.
5. Riavvia l'istanza con lo script originale.

Modifiche automatiche alla configurazione delle ist

L'automazione della configurazione delle istanze AMS Accelerate apporta le seguenti modifiche all'account:

1. Autorizzazioni IAM

   Aggiunge le politiche gestite da IAM necessarie per concedere all'istanza l'autorizzazione a utilizzare gli agenti installati da AMS Accelerate.

2. Agenti

   a. L' CloudWatch agente Amazon è responsabile dell'emissione dei log e dei parametri del sistema operativo. L'automazione della configurazione dell'istanza garantisce che l' CloudWatch agente sia installato ed esegua la versione minima di AMS Accelerate.

b. L'agente AWS Systems Manager SSM è responsabile dell'esecuzione dei comandi remoti sull'istanza. L'automazione della configurazione dell'istanza garantisce che l'agente SSM esegua la versione minima di AMS Accelerate.

3. CloudWatch Configurazione

a. Per garantire che vengano emessi i parametri e i log richiesti, AMS Accelerate personalizza la configurazione. CloudWatch Per ulteriori informazioni, consulta la sezione seguente,. CloudWatch dettagli di modifica della configurazione

La configurazione automatizzata delle istanze apporta modifiche o aggiunte ai profili e alla CloudWatch configurazione delle istanze IAM.

Dettagli della modifica delle autorizzazioni IAM

Ogni istanza gestita deve avere un AWS Identity and Access Management ruolo che includa le seguenti politiche gestite:

- arn:aws:iam: :aws:policy/Amazon SSMManaged InstanceCore
- arn:aws:iam: :aws:policy/ CloudWatchAgentServerPolicy
- arn:aws:iam: :aws:policy/ AMSInstance ProfileBasePolicy

Le prime due sono politiche gestite. AWS La policy gestita da AMS è la seguente:

AMSInstanceProfileBasePolicy

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "secretsmanager:CreateSecret",
                "secretsmanager:UpdateSecret"
            ],
            "Resource": [
                "arn:aws:secretsmanager:*:*:secret:/ams/byoa/*"
            ],
            "Effect": "Allow"
```

```
        },
        {
            "Action": [
                "kms:Encrypt"
            ],
            "Resource": [
                "*"
            ],
            "Effect": "Allow"
        }
    ]
}
```

Se alla tua istanza è già associato un ruolo IAM, ma manca una di queste policy, AMS aggiunge le policy mancanti al tuo ruolo IAM. Se la tua istanza non ha un ruolo IAM, AMS assegna il ruolo AMSOSConfigurationCustomerInstanceProfileIAM. Il ruolo AMSOSConfigurationCustomerInstanceProfileIAM ha tutte le politiche richieste da AMS Accelerate.

> **Note**
>
> Se viene raggiunto il limite predefinito del profilo di istanza di 10, AMS aumenta il limite a 20, in modo da poter allegare i profili di istanza richiesti.

CloudWatch dettagli di modifica della configurazione

Dettagli aggiuntivi sulla CloudWatch configurazione.

- CloudWatch posizione del file di configurazione sull'istanza:
  - Windows:%ProgramData%\ Amazon\AmazonCloudWatchAgent\ amazon-cloudwatch-agent .json
  - Linux:/-accelerate-config.json opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.d/ams
- CloudWatch posizione del file di configurazione in Amazon S3:
  - Windows: https://ams-configuration-artifacts- *REGION_NAME* .s3. *REGION_NAME*.amazonaws. com/configurations/cloudwatch/latest/windows-cloudwatch-config.json
  - Linux: https://- .s3. ams-configuration-artifacts *REGION_NAME REGION_NAME*.amazonaws. com/ configurations/cloudwatch/latest/linux-cloudwatch-config.json
- Metriche raccolte:

  - Windows:
    - AWS Systems Manager Agente SSM (CPU_Usage)
    - CloudWatch Agente (CPU_Usage)
    - Utilizzo dello spazio su disco per tutti i dischi (% spazio libero)
    - Memoria (% di byte impegnati in uso)
  - Linux:
    - AWS Systems Manager Agente SSM (CPU_Usage)
    - CloudWatch Agente (CPU_Usage)
    - CPU (cpu_usage_idle, cpu_usage_iowait, cpu_usage_user, cpu_usage_system)
    - Disco (used_percent, inodes_used, inodes_total)
    - Diskio (io_time, write_bytes, read_bytes, scrive, legge)
    - Mem (mem_used_percent)
    - Scambia (swap_used_percent)
- Registri raccolti:
  - Windows:
    - SSMAgentRegistro Amazon
    - AmazonCloudWatchAgentLog
    - SSMErrorRegistro Amazon
    - AmazonCloudFormationLog
    - ApplicationEventLog
    - EC2ConfigServiceEventLog
    - MicrosoftWindowsAppLockerEXEAndDLLEventRegistro
    - MicrosoftWindowsAppLockerMSIAndScriptEventLog
    - MicrosoftWindowsGroupPolicyOperationalEventLog
    - SecurityEventLog
    - SystemEventLog
  - Linux:
    - /var/log/amazon/ssm/amazon-ssm-agent.log
    - /var/log/amazon/ssm/errors.log

    - /.log var/log/audit/audit

- /-init-output.log var/log/cloud
- /var/log/cloud-init.log
- /var/log/cron
- /var/log/dpkg.log
- /var/log/maillog
- /var/log/messages
- /var/log/secure
- /var/log/spooler
- /var/log/syslog
- /.log var/log/yum
- /.log var/log/zypper

Offboard di AMS Accelerate

AMS Accelerate offre un modo semplice per gestire un ambiente operativo di livello aziendale. Inoltre, AMS Accelerate fornisce il modello operativo dell'infrastruttura di supporto per la AWS migrazione e l'utilizzo. Tuttavia, dopo aver utilizzato AMS Accelerate, potresti decidere di integrare o riassegnare le responsabilità operative AWS dell'infrastruttura ad altri team. A tale scopo, è necessario eliminare i propri account dal servizio AMS.

Quando trasferisci un account da AMS Accelerate, AMS ti trasferisce tutte le responsabilità definite nella nostra descrizione del servizio. Ad esempio, non avrai la possibilità di limitare gli incidenti o le richieste di assistenza ad AMS. Allo stesso modo, i nostri tecnici operativi e di automazione non avranno più accesso ai tuoi account Accelerate, il che ci impedisce di porre rimedio ai problemi di salute, disponibilità, sicurezza e conformità. I tuoi AWS carichi di lavoro possono continuare a funzionare negli stessi account utilizzati da AMS.

Il team che in futuro eseguirà i servizi operativi dell'infrastruttura deve essere incluso per definire quali persone, strumenti e processi utilizzerai dopo l'offboarding di Accelerate. AMS abbandona alcuni strumenti AMS, come guardrail e logs, per consentire lo sviluppo di un ambiente operativo e di un modello «futuri». Consulta attentamente la seguente documentazione per comprendere quali strumenti puoi continuare a utilizzare e come richiedere l'offboard di un account.

AMS Accelera gli effetti dell'offboarding

Mentre ti prepari ad abbandonare Accelerate, tieni a mente le seguenti considerazioni.

- Accesso: lo `ams-access-management` CloudFormation stack che definisce il `ams-access-management` AWS Identity and Access Management ruolo non viene eliminato. Dopo l'offboarding, queste risorse rimangono, ma non vengono utilizzate dagli altri componenti rimasti. Puoi eliminare lo stack e il ruolo a tuo piacimento.
- Conservazione delle risorse AMS: dopo l'offboarding, alcune risorse AMS rimangono nel tuo account. Per vedere quali risorse vengono conservate e cosa puoi fare con esse, consulta il `resource_inventory.zip`foglio di calcolo (compresso).
- Automazione: dopo l'offboarding, i runbook di automazione AWS SSM e le funzioni AWS Lambda curati da AMS non sono più disponibili.
- Gestione dei backup: AMS utilizza la gestione dei backup per scattare istantanee delle risorse. Dopo l'offboarding, è possibile continuare a utilizzare i piani di backup, la frequenza e i periodi di conservazione definiti AWS Backup ad eccezione dei piani di backup AMS; vedere. Seleziona un piano di backup AMS Le AWS Identity and Access Management risorse create da AMS Backup Orchestrator vengono rimosse, ma non gli archivi di backup creati da AMS e la chiave corrispondente. AWS KMS Accelerate non monitora più i processi di backup né esegue azioni di ripristino durante gli incidenti.
- Ottimizzazione dei costi: dopo l'offboarding, AMS Resource Scheduler viene eliminato. AMS Resource Scheduler aiuta a ridurre i costi operativi bloccando le risorse non utilizzate e riavviandole quando è necessaria la loro capacità. AMS non continua a fornire raccomandazioni per l'ottimizzazione dei costi. Per i dettagli su Resource Scheduler, consulta Ottimizzazione dei costi con AMS Resource Scheduler.
- Esperti designati: dopo l'offboarding, il Cloud Service Delivery Manager (CSDM) e il Cloud Architect (CA) designati non forniscono più indicazioni, report o promuovono l'eccellenza operativa e di sicurezza per gli account Accelerate che non utilizzano più.
- Gestione degli incidenti: la gestione degli incidenti è il processo utilizzato dal servizio AMS per rispondere agli incidenti segnalati. Dopo l'offboarding, Accelerate non rileva e non risponde più agli incidenti né assiste il team nella risoluzione dei problemi. Non potrai scambiare comunicazioni relative a incidenti e richieste di assistenza con Accelerate e l'accesso alla console di Accelerate per i tuoi account Accelerate è disattivato.
- Registrazione e reportistica: dopo l'offboarding, conservi i log archiviati come risultato di CloudWatch, CloudTrail e VPC Flow Logs. È possibile lasciare la configurazione di tali servizi così com'è per continuare a generare i log; tuttavia, AMS non monitora più tali configurazioni.

Accelerate non fornisce più il rapporto mensile di servizio che riassume le metriche chiave delle prestazioni di AMS. I dati generati da Self-Service Reporting (SSR) vengono conservati (vediReport self-service), ma Accelerate non ne genera di nuovi.

- Monitoraggio: il monitoraggio è il processo utilizzato dal servizio AMS per tenere traccia delle risorse. Durante l'offboarding, AMS rimuove gli strumenti specifici di AMS, come Alarm Manager e Resource Tagger, e tutte le regole e gli CloudWatch allarmi relativi agli EventBridge eventi che AMS ha implementato come parte della linea di base di monitoraggio AMS. Accelerate non risponderà più agli allarmi né ne configurerà di nuovi dopo l'offboarding. Per i dettagli su Alarm Manager e Resource Tagger, consulta Alarm Manager basato su tag e Resource Tagger.
- Strumenti operativi: AMS Accelerate può fornire operazioni continue per l'infrastruttura del carico di lavoro in AWS. Dopo l'offboarding di un account Accelerate, non hai più accesso a strumenti come Resource Tagger, che ti aiuta a etichettare le tue risorse in base a regole, o la configurazione automatica delle istanze per installare gli agenti necessari nelle tue istanze. EC2 CloudWatch e gli agenti SSM sulle istanze rimangono invariati con le configurazioni esistenti. Il profilo `AMSOSConfigurationCustomerInstanceRole` IAM e il `AMSInstanceProfileBasePolicy` vengono scollegati dalle istanze e rimossi dagli account Accelerate.
- Gestione delle patch: la gestione delle patch è il processo utilizzato dal servizio AMS per aggiornare le EC2 istanze. Dopo l'offboarding, AMS non crea più un'istantanea dell'istanza prima dell'applicazione delle patch, non installa e non monitora più l'installazione delle patch e non notifica più all'utente il risultato. Conservate le linee di base e le istantanee della patch create in passato. Inoltre, la configurazione delle finestre di manutenzione delle patch rimane invariata, ma le patch non vengono più installate da Accelerate.
- Gestione dei problemi: dopo l'offboarding, Accelerate non esegue più analisi per identificare e analizzare i problemi e identificarne la causa principale.
- Sicurezza: la gestione della sicurezza è il processo utilizzato dal servizio AMS per proteggere le risorse. Dopo l'offboarding, conservi il GuardDuty rilevatore e i risultati di Amazon e tutte AWS Config le regole che hai creato. AWS Config le regole distribuite da Accelerate vengono rimosse. Accelerate non monitora, corregge o riporta più i risultati di questi strumenti.
- Data di cessazione del servizio: la data di cessazione del servizio è l'ultimo giorno del mese di calendario successivo alla fine del periodo di preavviso di risoluzione richiesto di 30 giorni. Se la fine del periodo di disdetta richiesto cade dopo il ventesimo giorno del mese solare, la data di cessazione del servizio è l'ultimo giorno del mese di calendario successivo. Di seguito sono riportati alcuni esempi di scenari relativi alle date di cessazione.
  - Se l'avviso di risoluzione viene fornito il 12 aprile, il preavviso di 30 giorni termina il 12 maggio. La data di cessazione del servizio è il 31 maggio.

- Se viene fornito un avviso di risoluzione il 29 aprile, il preavviso di 30 giorni termina il 29 maggio. La data di cessazione del servizio è il 30 giugno.

Offboarding da AMS Accelerate con dipendenza da Alarm Manager e Resource Tagger

CloudFormation Gli stack personalizzati che implementano configurazioni relative ad Alarm Manager o Resource Tagger, insieme agli stack di configurazione Alarm Manager e Resource Tagger forniti da AMS, rimangono nel tuo account quando esci da AWS Managed Services.

Per eliminare gli stack di configurazione AMS durante il processo di offboarding, è necessario rimuovere qualsiasi dipendenza e riferimento da Alarm Manager o Resource Tagger dai modelli personalizzati prima di avviare il processo di offboarding. CloudFormation La rimozione dei riferimenti aiuta a garantire che gli stack vengano rimossi correttamente dal tuo account quando esci da AMS.

> **Important**
>
> Esamina attentamente i CloudFormation modelli e rimuovi qualsiasi riferimento ad Alarm Manager e Resource Tagger prima di iniziare il processo di offboarding. In caso contrario, questi stack potrebbero rimanere memorizzati nel tuo account, anche dopo aver lasciato AMS. Tieni presente che, sebbene questi stack contengano informazioni di configurazione specifiche per Alarm Manager e Resource Tagger, la loro presenza non comporta costi o commissioni correnti.

Ottenere assistenza per l'offboarding per un account Accelerate

AMS trasferisce il tuo account dopo aver ricevuto un preavviso di almeno 30 giorni tramite una richiesta di chiusura del servizio di account AMS. La data di cessazione del servizio è l'ultimo giorno del mese di calendario successivo alla fine del periodo di preavviso di risoluzione richiesto di 30 giorni; a condizione che, se la fine del periodo di disdetta richiesto cade dopo il ventesimo giorno del mese solare, la data di cessazione del servizio sarà l'ultimo giorno del mese di calendario successivo.

Per richiedere la disattivazione di un account devi:

1. Invia una richiesta formale di trasferimento dall'account utilizzando una richiesta di servizio. Una richiesta di servizio (SR) che documenti tutti gli account che desideri trasferire o una richiesta di assistenza per account.

Nella richiesta, fornisci l'elenco degli account IDs da eliminare, il motivo dell'abbandono ed eventuali considerazioni aggiuntive.

2. Informa il CSDM sugli account che desideri eliminare dall'imbarco e richiedi il loro aiuto per l'esecuzione della procedura di offboarding.

Impostazioni di notifica in Accelerate

Le comunicazioni tra l'utente e AMS avvengono per diverse ragioni:

- Eventi creati dagli avvisi di monitoraggio
- Notifiche del servizio di patch, se hai attivato il componente aggiuntivo Patch
- Richieste di assistenza e segnalazioni di incidenti
- AWS Annunci occasionali importanti (il CSDM vi contatterà se è necessaria un'azione da parte vostra)

Tutte le notifiche vengono inviate utilizzando un'e-mail che avete fornito per le notifiche sulle patch al momento dell'onboarding. Altrimenti, le notifiche vengono inviate all'e-mail predefinita che hai fornito ad AMS al momento dell'onboarding. Poiché è difficile mantenere aggiornate le singole e-mail, ti consigliamo di utilizzare un'e-mail di gruppo che possa essere aggiornata da parte tua. Tutte le notifiche che ti vengono inviate vengono ricevute anche dalle operazioni AMS e analizzate prima di dare una risposta.

È possibile utilizzare elenchi di contatti denominati per notifiche non basate su risorse, ad esempio avvisi basati su o GuardDuty AWS Config. Ad esempio, potresti avere un elenco denominato `SecurityContacts` e un altro denominato. `OperationsContacts` AMS invia allarmi e notifiche a questi elenchi.

Per ulteriori dettagli, consulta AWS Config Rapporto di controllo della conformità.

Etichettatura in AMS Accelerate

La maggior parte delle funzionalità di Accelerate (applicazione di patch, backup, monitoraggio) utilizza tag e profili di configurazione per decidere quali risorse gestire, quali azioni applicare e quando applicarle. I tag sono etichette che si applicano alle risorse. I profili di configurazione contengono regole basate su tali tag.

Ogni funzionalità di Accelerate ha i propri requisiti di etichettatura. Alcune funzionalità richiedono l'utilizzo di tag specifici, mentre altre consentono di utilizzare tag personalizzati.

Per informazioni sui tag obbligatori, consultaTag gestiti dai clienti in Accelerate.

Per informazioni sui tag che possono essere definiti clienti, vedere Tag forniti dal cliente in Accelerate

Indice

- Tag in AMS Accelerate
  - Cosa sono i tag?
  - Come funziona il tagging
  - Tag gestiti dai clienti in Accelerate
    - Monitoraggio in Accelere
    - Configurazione dei tag per le EC2 istanze in Accelerate
    - Gestione dei tag per i backup in Accelerate
  - Tag con gestione accelerata
  - Tag forniti dal cliente in Accelerate
- Strumenti di gestione dei tag per Accelerate
  - Accelera Resource Tagger
    - Che cos'è Resource Tagger?
    - Come funziona Resource Tagger
    - Profili di configurazione Resource Tagger in AMS Accelerate
      - Sintassi e struttura
    - Casi d'uso Resource Tagger in AMS Accelerate
      - Visualizzazione dei tag applicati da Resource Tagger
      - Utilizzo di Resource Tagger per creare tag
      - Impedire a Resource Tagger di modificare le risorse

        - Esempio di profilo di configurazione
        - Unire la configurazione predefinita
        - Disabilitazione della configurazione predefinita
        - Rimozione dei tag applicati da Resource Tagger
        - Visualizzazione o modifica della configurazione di Resource Tagger
        - Implementazione delle modifiche alla configurazione
        - Configurazione di Terraform per ignorare i tag Resource Tagger
        - Visualizzazione del numero di risorse gestite da Resource Tagger
- Utilizzo CloudFormation per creare tag per AMS Accelerate
    - CloudFormation Casi d'uso per AMS Accelerate
        - Taggare un' EC2 istanza con CloudFormation for Accelerate
        - Taggare un AutoScaling gruppo (ASG) con CloudFormation For Accelerate
        - Implementazione di un profilo di configurazione con CloudFormation for Accelerate
- Utilizzo di Terraform per creare tag per AMS Accelerate

Tag in AMS Accelerate

Indice

- Cosa sono i tag?
- Come funziona il tagging
- Tag gestiti dai clienti in Accelerate
    - Monitoraggio in Accelere
    - Configurazione dei tag per le EC2 istanze in Accelerate
    - Gestione dei tag per i backup in Accelerate
- Tag con gestione accelerata
- Tag forniti dal cliente in Accelerate

Cosa sono i tag?

Un tag è un'etichetta che si assegna a una AWS risorsa. Ogni tag è composto da una chiave e da un valore opzionale, entrambi personalizzabili.

I tag vengono utilizzati per classificare le AWS risorse in diversi modi, ad esempio per scopo, proprietario o ambiente. Ad esempio, puoi definire un set di tag per le EC2 istanze Amazon del tuo account, che ti aiutano a monitorare il proprietario e il livello di stack di ogni istanza.

I tag non hanno alcun significato semantico per Amazon EC2 e vengono interpretati rigorosamente come una stringa di caratteri.

Per ulteriori informazioni, consulta Taggare AWS le risorse.

Come funziona il tagging

Esistono diversi modi per applicare i tag alle risorse. Puoi taggare le risorse direttamente nella console di ogni AWS servizio al momento della creazione della risorsa, utilizzare AWS Tag Editor per aggiungere, rimuovere o modificare i tag per più risorse o utilizzare strumenti di provisioning come CloudFormation Resource tag. AMS Accelerate fornisce anche l'AMS Accelerate Resource Tagger che puoi utilizzare per definire le regole per un gestore automatico del ciclo di vita dei tag. Per informazioni sull'utilizzo di Resource Tagger in AMS Accelerate, consulta. Accelera Resource Tagger AMS Accelerate fornisce anche tag forniti dal cliente per aggiungere e rimuovere tag personalizzati dalle risorse AMS. Per ulteriori informazioni sui tag forniti dal cliente, consulta. Tag forniti dal cliente in Accelerate

Tag gestiti dai clienti in Accelerate

Alcuni tag sono necessari per attivare varie azioni di AMS Accelerate.

Indice

- Monitoraggio in Accelere
- Configurazione dei tag per le EC2 istanze in Accelerate
- Gestione dei tag per i backup in Accelerate

Monitoraggio in Accelere

AMS Accelerate monitora lo stato, la disponibilità e l'affidabilità delle risorse supportate. Per ulteriori informazioni su questa offerta di servizi, consultaMonitoraggio e gestione degli eventi in AMS Accelerate.

AMS Accelerate effettua periodicamente integrazioni aggiuntive rispetto Servizi AWS al monitoraggio di base. Se utilizzi la configurazione predefinita di Resource Tagger, questi aggiornamenti vengono distribuiti automaticamente ai tuoi account e le modifiche si riflettono sulle risorse supportate.

Per attivare la gestione EC2 delle tue istanze Amazon da AMS Accelerate, devi applicare il seguente tag tramite il profilo di personalizzazione in AppConfig; per ulteriori informazioni, consulta la Fase 3: Creazione di una configurazione e di un profilo di configurazione.

Applica il seguente tag alle tue risorse:

Chiave	Valore
ams:rt:ams-managed	true

Ad esempio, puoi creare un documento di configurazione personalizzato come questo per applicare i tag a tutte le risorse supportate da AMS EC2 :

```
{
    "AWS::EC2::Instance": {
        "AllEC2": {
            "Enabled": true,
            "Filter": {
                "Platform": "*"
            },
            "Tags": [
                {
                    "Key": "ams:rt:ams-managed",
                    "Value": "true"
                }
            ]
        }
    }
}
```

Important

Ricordati di implementare le modifiche alla configurazione dopo averle apportate. In SSM AppConfig, è necessario distribuire una nuova versione della configurazione dopo averla creata.

I servizi diversi da Amazon EC2 avranno un monitoraggio di base predefinito. Per disattivare il monitoraggio delle risorse da parte di AMS Accelerate, puoi utilizzare il profilo di configurazione di

personalizzazione per escludere risorse specifiche oppure. Servizi AWS Ciò consente di controllare quali risorse devono avere tag di monitoraggio per implementare le definizioni di allarmi di base. Per informazioni, consulta Casi d'uso Resource Tagger in AMS Accelerate.

Utilizzo di Resource Tagger

La configurazione AMS Accelerate Resource Tagger nel tuo account aiuta a garantire che i seguenti tag vengano distribuiti automaticamente, se applichi questo unico tag (ams:rt:ams-managed).

Vedrai i seguenti tag applicati alle risorse supportate per il monitoraggio di base.

Chiave	Valore	Regola
ams: rt: ams-monitoring-policy	sono monitorati	Si applica a tutte le EC2 risorse supportate da AMS
ams: rt: ams-monitoring-pol icy-platform	ams-monitored-linux	Si applica a tutte le EC2 istanze Amazon che eseguono il sistema operativo Linux
ams: rt: ams-monitoring-pol icy-platform	ams-monitored-windows	Si applica a tutte le EC2 istanze Amazon che eseguono il sistema operativo Windows

Per altri servizi supportati

Applica i seguenti tag alle tue risorse, secondo le regole fornite:

Chiave	Valore	Regola
ams: rt: ams-monitoring-policy	sono monitorati	Si applica a tutte le risorse supportate dal monitoraggio di AMS Accelerate.
ams: rt: ams-monitoring-with-kms	ams-monitored-with-kms	OpenSearch Dominio con KMS
ams: rt: ams-monitoring-with-master	ams-monitored-with-master	OpenSearch Dominio con nodo master dedicato

Se non utilizzi Resource Tagger

Consulta Accelera i tag senza Resource Tagger per assistenza sull'applicazione dei tag di monitoraggio corretti utilizzando metodi diversi dall'utilizzo di AMS Resource Tagger.

Configurazione dei tag per le EC2 istanze in Accelerate

AMS Accelerate gestisce gli agenti sulle tue EC2 istanze Amazon, come l'agente SSM e l' CloudWatch agente. Per ulteriori informazioni su questa offerta di servizi, consulta Configurazione automatica delle istanze in AMS Accelerate

Per attivare la gestione EC2 delle tue istanze Amazon da AMS Accelerate, devi applicare il seguente tag alle tue istanze Amazon EC2 :

Chiave	Valore
ams:rt:ams-managed	true

Gestione dei tag per i backup in Accelerate

AMS Accelerate gestisce il backup delle risorse supportate. Per ulteriori informazioni su questa offerta di servizi, consultaGestione della continuità in AMS Accelerate.

La gestione dei backup di AMS Accelerate utilizza i tag per identificare quali risorse devono essere sottoposte a backup automatico (e fornisce anche funzionalità di backup manuale). Puoi utilizzare qualsiasi combinazione di tag chiave:valore per associare le tue risorse ai piani di backup. Per attivare i backup automatici utilizzando il ams-default-backup-plan AWS Backup piano, devi applicare il seguente tag alle risorse supportate:

Chiave	Valore
ams:rt:backup-orchestrator	true

> **Note**
>
> Durante l'onboarding, AMS Accelerate etichetta tutte le risorse con ams:rt: backup-orchestrator-onboarding with value true per istantanee a breve intervallo e di conservazione

brevi. Questo è gestito dal piano di backup. ams-onboarding-backup-plan Per ulteriori informazioni sui AWS Backup piani gestiti da AMS Accelerate, consulta. Seleziona un piano di backup AMS

Tag con gestione accelerata

Durante l'onboarding su AMS Accelerate, diverse AWS risorse vengono distribuite sul tuo account. Per consentirti di identificarle, queste risorse sono contrassegnate con quanto segue:

Chiave	Valore
AMS: proprietario della risorsa	AMS
obiettivi: resourceOwnerService	Una descrizione del servizio AMS Accelerate che offre questa risorsa proviene, ad esempio, da AMS Deployment, Backup, Controls, Monitoring, Patch e così via.
AppId	AMSInfrastructure
AppName	
Ambiente	

Note

Questi tag vengono applicati utilizzando tag a CloudFormation livello di stack e si basano sulla CloudFormation propagazione dei tag alle risorse create. Per ulteriori informazioni, consulta Resource tag.

Tag forniti dal cliente in Accelerate

Cosa sono i tag forniti dal cliente?

I tag forniti dal cliente sono una funzionalità del servizio AMS Accelerate utilizzata per specificare le regole che regolano il modo in cui le risorse AMS vengono taggate nell'account. Con i tag forniti

dal cliente, puoi aggiungere tag personalizzati definiti dall'utente alle risorse AMS distribuite nei tuoi account. La funzionalità dei tag forniti dal cliente viene aggiunta automaticamente agli account richiesti quando effettui la richiesta al Cloud Service Delivery Manager (CSDM) utilizzando un servizio automatizzato. Tieni presente che non puoi sovrascrivere i tag AMS. I tag AMS iniziano con 'ams: '.

Puoi definire i tuoi tag (etichette) e specificare le funzionalità di questi tag per tutte le tue risorse AMS Accelerate. Puoi fornire questi tag prima di effettuare l'onboarding in AMS in modo che i tag AMS e i tag personalizzati vengano applicati durante il processo di onboarding. In alternativa, puoi fornire i tag dopo l'onboarding.

Come posso aggiungere tag forniti dal cliente?

Per richiedere l'aggiunta di questi tag alle tue risorse, contatta il tuo CSDM. Questi tag verranno applicati alle risorse AMS del tuo account.

Qual è lo scopo dei tag?

Questa funzionalità è attualmente disponibile solo per i clienti Accelerate e nelle regioni AWS commerciali. Puoi aggiungere tag a tutti gli account di tua proprietà o a un elenco specifico di account.

> **Note**
>
> Questi tag si applicano solo alle risorse AMS e non influiscono sulle tue risorse.

Strumenti di gestione dei tag per Accelerate

Indice

- Accelera Resource Tagger
- Utilizzo CloudFormation per creare tag per AMS Accelerate
- Utilizzo di Terraform per creare tag per AMS Accelerate

Accelera Resource Tagger

Con Resource Tagger, puoi specificare le regole per regolare il modo in cui AWS le risorse vengono taggate nel tuo account. Durante l'onboarding di un account, AMS Accelerate implementa la vostra politica di tagging per garantire che le risorse all'interno degli account gestiti siano etichettate.

Indice

- Che cos'è Resource Tagger?
- Come funziona Resource Tagger
- Profili di configurazione Resource Tagger in AMS Accelerate
  - Sintassi e struttura
- Casi d'uso Resource Tagger in AMS Accelerate
  - Visualizzazione dei tag applicati da Resource Tagger
  - Utilizzo di Resource Tagger per creare tag
  - Impedire a Resource Tagger di modificare le risorse
  - Esempio di profilo di configurazione
  - Unire la configurazione predefinita
  - Disabilitazione della configurazione predefinita
  - Rimozione dei tag applicati da Resource Tagger
  - Visualizzazione o modifica della configurazione di Resource Tagger
  - Implementazione delle modifiche alla configurazione
  - Configurazione di Terraform per ignorare i tag Resource Tagger
  - Visualizzazione del numero di risorse gestite da Resource Tagger

Che cos'è Resource Tagger?

Resource Tagger è un servizio AMS Accelerate che ti consente di specificare le regole per regolare il modo in cui AWS le risorse vengono taggate nel tuo account. Mira a fornirti una visibilità completa su come i tag vengono applicati alle tue AWS risorse.

Resource Tagger crea, aggiorna ed elimina automaticamente i tag sulle AWS risorse supportate, in base alle regole di tagging specificate nei profili di configurazione. Ad esempio, puoi specificare una regola che applica un tag a una raccolta di EC2 istanze Amazon, indicando che devono essere gestite da AMS Accelerate, il che comporta il monitoraggio o il backup delle istanze. Puoi utilizzare tag come questi per identificare lo stato di conformità delle AWS risorse in base alla politica definita nei tuoi profili di AWS AppConfig configurazione. Per ulteriori informazioni, consulta AWS AppConfig.

AMS Accelerate fornisce una configurazione di tagging gestita predefinita in modo da poter monitorare le risorse da AMS Accelerate. Siete voi a definire quali risorse devono essere gestite da

AMS Accelerate e le regole di tagging gestite assicurano che le risorse con i tag appropriati vengano monitorate da AMS Accelerate.

Con Resource Tagger, se lo desideri, puoi sovrascrivere o disattivare i tag gestiti predefiniti di AMS Accelerate, fornire le tue regole di tagging per soddisfare le tue politiche e utilizzare altri meccanismi, come Terraform, per evitare deviazioni. Puoi definire le eccezioni da scalare, in base alle tue operazioni. Ad esempio, puoi definire una policy per applicare i tag a tutte le EC2 istanze Amazon con piattaforme supportate (come Windows e Linux) ed escluderle dall'etichettatura di istanze specifiche. IDs

> **Important**
>
> Resource Tagger controlla tutti i tag del tuo account che hanno il prefisso ams:rt:. Tutti i tag che iniziano con questo prefisso vengono eliminati a meno che non siano presenti nelle regole di configurazione di Resource Tagger. Riassumendo, qualsiasi tag sulle risorse supportate che inizia con ams:rt: è considerato di proprietà di Resource Tagger. Se tagghi manualmente qualcosa con, ad esempio, ams:rt:, quel tag verrebbe rimosso automaticamente se non fosse specificato in uno dei profili di configurazione di Resource Tagger.

Come funziona Resource Tagger

Quando il tuo account viene registrato su AMS Accelerate, nel tuo account vengono distribuiti due documenti di configurazione JSON in. AWS AppConfigI due documenti, denominati profili di configurazione, sono AMSManagedTag, indicati come profilo di configurazione predefinito CustomerManagedTags, e denominati profilo di configurazione di personalizzazione. Il profilo di configurazione di personalizzazione viene utilizzato per definire politiche e regole personalizzate per gli account, che non vengono sovrascritte da AMS Accelerate.

Entrambi i profili risiedono nell'applicazione AMSResourceTagger e nell'ambiente. AMSInfrastructure Tutti i tag applicati dal resource tagger hanno il prefisso chiave ams:rt:.

Profilo di configurazione di personalizzazione:

Il profilo di configurazione di personalizzazione è inizialmente vuoto al momento dell'onboarding dell'account; tuttavia, tutte le regole inserite nel documento del profilo vengono applicate, oltre alle regole del profilo di configurazione predefinito. Qualsiasi configurazione nel profilo di configurazione

di personalizzazione è gestita interamente dall'utente e non viene sovrascritta da AMS Accelerate, se non su richiesta dell'utente.

Puoi specificare tutte le regole di tagging personalizzate che desideri nel profilo di configurazione personalizzato per le AWS risorse supportate e puoi anche specificare le modifiche alla configurazione predefinita gestita da AMS Accelerate qui, vedi. Casi d'uso Resource Tagger in AMS Accelerate

> **Important**
>
> Se aggiorni questo profilo, Resource Tagger applica automaticamente le modifiche a tutte le risorse pertinenti del tuo. Account AWS Le modifiche vengono applicate automaticamente, ma possono essere necessari fino a 60 minuti per diventare effettive.

È possibile aggiornare questo profilo utilizzando o tramite Console di gestione AWS gli strumenti AWS CLI/SDK. Per informazioni sull'aggiornamento di un profilo di configurazione di personalizzazione, consulta la guida per l' AWS AppConfig utente: What Is? AWS AppConfig

Profilo di configurazione predefinito:

Il documento del profilo di configurazione predefinito è interno ad AMS Accelerate e contiene regole predefinite fornite da AMS Accelerate che non è possibile modificare o eliminare in modo permanente. Questo profilo può essere aggiornato in qualsiasi momento da AMS Accelerate e reso disponibile per la revisione; tutte le modifiche apportate vengono eliminate automaticamente. Se desideri modificare o disabilitare una qualsiasi delle regole di configurazione predefinite, utilizza il profilo di configurazione di personalizzazione, consultaCasi d'uso Resource Tagger in AMS Accelerate.

Profili di configurazione Resource Tagger in AMS Accelerate

I profili di configurazione aiutano a garantire che i tag vengano applicati in modo uniforme alle risorse per tutta la durata delle risorse.

Sintassi e struttura

Un profilo di configurazione è un oggetto JSON con la seguente struttura:

```
{
   "Options": {
      "ReadOnly": false
```

```
   },
   "ResourceType": {
      "ConfigurationID": {
      "Enabled": true,
      "Filter": { ... },
      "Tags": [  ...  ]
      },
      "ConfigurationID": {
      ...
      }
   },
   "ResourceType": {
     ...
   }
}
```

Opzioni: (opzionale) Specificate le opzioni per il modo in cui desiderate che ResourceTagger si comporti. Omettere il blocco equivale a impostare tutte le opzioni sui valori predefiniti. Vedi sotto per le impostazioni delle opzioni disponibili:

- ReadOnly: (opzionale, il valore predefinito è false): specifica la ReadOnly modalità per Resource Tagger. Imposta su true ReadOnly per disabilitare Resource Tagger che crea o rimuove tag sulle risorse AWS. Per ulteriori informazioni, consulta Impedire a Resource Tagger di modificare le risorse.

ResourceType: Questa chiave deve essere una delle seguenti stringhe supportate e rappresenta tutte le configurazioni relative al tipo di risorsa indicato:

- AWS::AutoScaling::AutoScalingGruppo
- AWS::DynamoDB::Table
- AWS::EC2::Instance
- AWS::EC2::NatGateway
- AWS:EC2:: VPNConnection
- AWS::EFS::FileSystem
- AWS::EKS::Cluster
- AWS::ElasticLoadBalancing::LoadBalancer
- AWS::ElasticLoadBalancingV2::LoadBalancer
- AWS::Elasticsearch::Domain

- AWS::FSx::FileSystem
- AWS::OpenSearch::Domain
- AWS: :RDS:: DBCluster
- AWS: :RDS:: DBInstance
- AWS::Redshift::Cluster
- AWS::S3::Bucket
- AWS::Synthetics::Canary

ConfigurationID: questa chiave deve essere univoca nel documento del profilo e denominare in modo univoco il seguente blocco di configurazione. Se due blocchi di configurazione nello stesso ResourceTypeblocco hanno lo stesso ConfigurationID, quello che appare per ultimo nel profilo ha effetto. Se si specifica un ConfigurationID nel profilo di personalizzazione che è lo stesso specificato nel documento predefinito, il blocco di configurazione definito nel profilo di personalizzazione ha effetto.

> **Important**
>
> Il ConfigurationID dovrebbe ***not***sovrapporsi al profilo AMS Accelerate; ad esempio, non dovrebbe essere AMSMonitoringLinux o AMSMonitoringWindows, altrimenti disabiliterà la rispettiva configurazione del profilo di configurazione Tags. AMSManaged

Abilitato (opzionale, il valore predefinito è true): specifica se il blocco di configurazione ha effetto. Imposta questo valore su false per disabilitare un blocco di configurazione. Un blocco di configurazione disabilitato non ha alcun effetto.

Filtro: specifica le risorse a cui si applica la configurazione. Ogni oggetto filtro può avere uno qualsiasi (ma solo uno) dei seguenti campi:

- AWS::AutoScaling::AutoScalingGruppo:
  - AutoScalingGroupName: il nome del gruppo Autoscaling. Questo campo supporta la corrispondenza con caratteri jolly.
- AWS::DynamoDB::Table:
  - TableName: il nome della tabella DynamoDB. Questo campo supporta la corrispondenza con caratteri jolly.
- AWS::EC2::Instance:

  - AvailabilityZone: il filtro corrisponde a un' EC2 istanza nella zona di disponibilità specificata. Questo campo supporta la corrispondenza con caratteri jolly, quindi *a corrisponde a us-east-1a, ap-northeast-1a e così via.
  - InstanceId: Il filtro corrisponde a un'istanza con l'ID di istanza specificato. EC2 Questo campo supporta la corrispondenza con caratteri jolly, quindi i-00000* corrisponderebbe a qualsiasi istanza con un ID di istanza che inizia con i-00000.
  - Piattaforma: il filtro abbina un' EC2 istanza alla piattaforma specificata. I valori validi sono windows, linux o la wildcard * (per corrispondere a qualsiasi piattaforma).
- AWS::EC2::NatGateway:
  - NatGatewayId: L'ID del gateway NAT. Questo campo supporta la corrispondenza con caratteri jolly.
  - Stato: lo stato del gateway NAT (in sospeso | non riuscito | disponibile | in eliminazione | eliminato o con carattere jolly «*»)
  - VpcId: L'ID del VPC in cui risiede il gateway NAT. Questo campo supporta la corrispondenza con caratteri jolly.
  - SubnetId: L'ID della sottorete in cui risiede il gateway NAT. Questo campo supporta la corrispondenza con caratteri jolly
- AWS:EC2:: VPNConnection:
  - VpnConnectionId: L'ID della connessione. Questo campo supporta la corrispondenza con caratteri jolly.
- AWS::EFS::FileSystem:
  - FileSystemId: l'ID del file system EFS. Questo campo supporta la corrispondenza con caratteri jolly.
- AWS::EKS::Cluster:
  - ClusterName: nome del cluster. Questo campo supporta la corrispondenza con caratteri jolly.
- AWS::ElasticLoadBalancing::LoadBalancer (Classic Load Balancer):
  - LoadBalancerName: Il LoadBalancer nome. Questo campo supporta la corrispondenza con caratteri jolly.
  - Schema: può essere «rivolto a Internet», «interno» o con caratteri jolly «*».
  - VPCId: L'elemento VPCId in cui è installato il loadbalancer può essere un carattere jolly «*».
- AWS::ElasticLoadBalancingV2::LoadBalancer (Application Load Balancer (ALB)):
  - LoadBalancerArn: LoadBalancer Amazon Resource Name (ARN)

  - DNSName: La DNSName delle. LoadBalancer Questo campo supporta la corrispondenza con caratteri jolly.
  - LoadBalancerName: Il LoadBalancer nome. Questo campo supporta la corrispondenza con caratteri jolly.
- AWS::Elasticsearch::Domain:
  - DomainId: La ElasticSearch fonte DomainId della risorsa. Questo campo supporta la corrispondenza con caratteri jolly.
  - DomainName: La ElasticSearch fonte DomainName della risorsa. Questo campo supporta la corrispondenza con caratteri jolly.
  - HasMasterNode: valore booleano vero o falso. Corrisponde se il dominio ha un nodo master dedicato.
  - HasKmsKeyValore booleano vero o falso. Corrisponde se il dominio ha una chiave KMS per la crittografia a riposo.
- AWS::FSx::FileSystem:
  - FileSystemId: L'ID del FSx filesystem. Questo campo supporta la corrispondenza con caratteri jolly.
- AWS::OpenSearch::Domain:
  - DomainId: La OpenSearch fonte DomainId della risorsa. Questo campo supporta la corrispondenza con caratteri jolly.
  - DomainName: La OpenSearch fonte DomainName della risorsa. Questo campo supporta la corrispondenza con caratteri jolly.
  - HasMasterNode: Boolean; Se il dominio ha un nodo master dedicato, questo può essere impostato su true.
  - HasKmsKey: Se il dominio ha una chiave KMS per la crittografia a riposo, questa può essere impostata su true.
- AWS: :RDS:: DBCluster
  - DBClusterIdentificatore: il filtro abbina un identificatore del cluster RDS all'identificatore specificato. Questo campo non supporta la corrispondenza con caratteri jolly, pertanto è necessario specificare un identificatore di cluster.
  - Motore: il motore utilizzato dall'istanza RDS. Questo campo supporta la corrispondenza con caratteri jolly.
  - EngineVersion: La versione del motore. Questo campo supporta la corrispondenza con caratteri jolly.

- AWS: :RDS:: DBInstance
  - DBInstanceIdentificatore: il filtro corrisponde a un'istanza RDS con l'ID di istanza specificato. Questo campo non supporta la corrispondenza con caratteri jolly, pertanto è necessario specificare un identificatore di istanza.
  - Motore: il motore utilizzato dall'istanza RDS. Questo campo supporta la corrispondenza con caratteri jolly.
  - EngineVersion: La versione del motore. Questo campo supporta la corrispondenza con caratteri jolly.
- AWS::Redshift::Cluster:
  - ClusterIdentifier: L'identificatore del cluster. Questo campo supporta la corrispondenza con caratteri jolly.
- AWS::S3::Bucket:
  - BucketName: il nome del bucket S3. Questo campo supporta la corrispondenza con caratteri jolly.
- AWS::Synthetics::Canary:
  - CanaryName: Il nome del canarino Synthetics.

Altre proprietà del filtro:

- Tag: il filtro si applica a qualsiasi risorsa a cui è già applicato il tag specificato. Il valore di questa proprietà deve essere un oggetto JSON con i seguenti campi:
  - Chiave: deve essere una stringa esatta e specifica che le risorse devono avere un tag con quella chiave esatta.
  - Valore: specifica il valore corrispondente per il tag. Supporta i caratteri jolly, quindi un valore di Sample corrisponde a qualsiasi valore che termina con la stringa Sample.
- Fn: :AND: un array JSON di oggetti JSON. Ogni oggetto segue le stesse regole del blocco di configurazione Filter. Ciò specifica che il filtro corrisponde a qualsiasi risorsa che corrisponde a tutti i sottofiltri.
- Fn: :OR: un array JSON di oggetti JSON. Ogni oggetto segue le stesse regole del blocco di configurazione Filter. Ciò specifica che il filtro corrisponde a qualsiasi risorsa che corrisponde a uno qualsiasi dei sottofiltri.
- Fn: :NOT: Un oggetto JSON che segue le stesse regole del blocco di configurazione Filter. Ciò specifica che il filtro non corrisponde esplicitamente a nessuna risorsa che corrisponda al sottofiltro. Utilizzatelo per specificare le esclusioni dalle regole di etichettatura.

Tag: i tag da applicare alle risorse corrispondenti. (Vedi Convenzioni di denominazione e utilizzo dei tag.) Questo campo è un array di coppie chiave-valore:

- Chiave: la chiave del tag da applicare.
- Valore: il valore del tag da applicare.

> **Note**
>
> I tag applicati da Resource Tagger hanno sempre chiavi che iniziano con ams:rt:. Se non specifichi questo prefisso nel tuo profilo, Resource Tagger lo inserisce automaticamente. In questo modo Resource Tagger distingue i tag che possiede e gestisce dai tag utilizzati da altri strumenti per altri scopi.

Casi d'uso Resource Tagger in AMS Accelerate

Questa sezione elenca le azioni più comuni eseguite con Resource Tagger.

Visualizzazione dei tag applicati da Resource Tagger

Tutti i tag applicati da Resource Tagger hanno il prefisso chiave ams:rt:. Ad esempio, la seguente definizione di tag restituisce un tag con la chiave ams:rt:SampleKey e il valore sampleValue. Tutti i tag con questo prefisso vengono considerati parte di Resource Tagger.

```
{
 "Key": "sampleKey",
 "Value": "sampleValue"
}
```

> **Important**
>
> Se crei manualmente il tuo tag con il prefisso ams:rt:, viene considerato gestito da Resource Tagger. Ciò significa che se la risorsa è gestita da Resource Tagger, ma i profili di configurazione non indicano che il tag debba essere applicato, Resource Tagger rimuove il tag aggiunto manualmente. Se etichettate manualmente le risorse gestite da Resource Tagger, non utilizzate il prefisso ams:rt: per le chiavi dei tag.

Utilizzo di Resource Tagger per creare tag

L'AMS Accelerate Resource Tagger è un componente che viene distribuito nel tuo account durante l'onboarding di AMS Accelerate. Resource Tagger dispone di un set di regole configurabili che definiscono come etichettare le risorse, quindi applica tali regole, aggiungendo e rimuovendo automaticamente i tag sulle risorse per garantire che siano conformi alle tue regole.

Se desideri utilizzare Resource Tagger per etichettare le tue risorse, consulta. Accelera Resource Tagger

Di seguito è riportato un esempio di frammento di configurazione Resource Tagger che aggiunge il tag ams:rt:ams-managed con il valore true per tutte le istanze Amazon. EC2 Il tag ams:rt:ams-managed ti consente di far monitorare le tue risorse da AMS Accelerate.

```
{
    "AWS::EC2::Instance": {
        "SampleConfigurationBlock": {
            "Enabled": true,
            "Filter": {
                "Platform": "*"
            },
            "Tags": [
                {
                    "Key": "ams:rt:ams-managed",
                    "Value": "true"
                }
            ]
        }
    }
}
```

Warning

Fai attenzione quando specifichi il nome per la tua nuova configurazione (`SampleConfigurationBlock`nell'esempio fornito) poiché potresti inavvertitamente sovrascrivere la configurazione gestita da AMS con lo stesso nome.

Impedire a Resource Tagger di modificare le risorse

Resource Tagger può essere impostato su una modalità di sola lettura che impedisce l'aggiunta o la rimozione di tag sulle risorse. Ciò è utile se desideri fornire un meccanismo di tagging personalizzato.

In modalità di sola lettura, Resource Tagger esamina comunque le regole di tagging che vengono specificate nei profili di configurazione gestiti e del cliente ed esamina le risorse che non soddisfano queste regole di tagging. Tutte le risorse non conformi vengono visualizzate con. AWS Config Regole di AWS Config Quelle che puoi cercare hanno il prefisso. `AMSResourceTagger-` Ad esempio, la `AMSResourceTagger-EC2Instance` AWS Config regola valuta se vengono creati tag appropriati per `AWS::EC2::Instance` le risorse in base al profilo di configurazione.

Resource Tagger si ferma a questo punto e non apporta alcuna modifica alle risorse (non aggiunge o rimuove tag).

È possibile abilitare la modalità di sola lettura modificando il profilo di configurazione del cliente per includere la ReadOnlychiave nel blocco Opzioni. Ad esempio, il seguente frammento di profilo di configurazione mostra come potrebbe apparire:

```
{
    "Options": {
        "ReadOnly": true
    },
    "AWS::EC2::Instance": {
        [... the rest of your configuration ...]
    }
}
```

Resource Tagger reagirà a questa nuova configurazione non appena avrà terminato la distribuzione e interromperà l'aggiunta e la rimozione di tag sulle risorse.

> **Note**
>
> Per riattivare la modifica dei tag, modifica il ReadOnlyvalore in false o rimuovi completamente la chiave, poiché il valore predefinito è false.

Per ulteriori informazioni sull'impostazione delle opzioni, vedereSintassi e struttura, successivo.

Esempio di profilo di configurazione

Il seguente documento di profilo di esempio specifica che tutte le EC2 istanze di Windows che fanno parte di uno CloudFormation stack stack-* devono essere gestite da AMS Accelerate; tuttavia, esclude esplicitamente una particolare istanza con ID i-00000000000000001. EC2

```
{
    "AWS::EC2::Instance": {
        "AMSMonitoringWindows": {
            "Enabled": true,
            "Filter": {
                "Fn::AND": [
                    {
                        "Platform": "Windows"
                    },
                    {
                        "Tag": {
                            "Key": "aws:cloudformation:stack-name",
                            "Value": "stack-*"
                        }
                    },
                    {
                        "Fn::NOT": {
                            "InstanceId": "i-00000000000000001"
                        }
                    }
                ]
            },
            "Tags": [
                {
                    "Key": "ams:rt:ams-managed",
                    "Value": "true"
                }
            ]
        }
    }
}
```

> **Warning**
>
> Fai attenzione quando specifichi il nome per la tua nuova configurazione (nell'esempio fornito) poiché potresti inavvertitamente sovrascrivere la configurazione `SampleConfigurationBlock` gestita da AMS con lo stesso nome.

Unire la configurazione predefinita

Il profilo di configurazione predefinito viene fornito da AMS Accelerate al momento dell'onboarding dell'account. Questo profilo fornisce regole predefinite che vengono implementate nel tuo account.

Sebbene non sia possibile modificare il profilo di configurazione predefinito, è possibile sostituire i valori predefiniti specificando un blocco di configurazione nel profilo di configurazione di personalizzazione con lo stesso ConfigurationID del blocco di configurazione predefinito. In tal caso, il blocco di configurazione sovrascrive il blocco di configurazione predefinito.

Ad esempio, considera il seguente documento di configurazione predefinito:

```
{
 "AWS::EC2::Instance": {
  "AMSManagedBlock1": {
   "Enabled": true,
   "Filter": {
    "Platform": "Windows"
   },
   "Tags": [{
    "Key": "my-tag",
    "Value": "SampleValueA"
   }]
  }
 }
}
```

Per modificare il valore del tag applicato qui da `SampleValueA` a `SampleValueB` e fare in modo che il tag venga applicato a tutte le istanze, non solo a quelle di Windows, è necessario fornire il seguente profilo di configurazione di personalizzazione:

```
{
 "AWS::EC2::Instance": {
```

```
  "AMSManagedBlock1": {
   "Enabled": true,
   "Filter": {
    "Platform": "*"
   },
   "Tags": [{
    "Key": "my-tag",
    "Value": "SampleValueB"
   }]
  }
 }
}
```

> **Important**
>
> Ricordati di distribuire le modifiche alla configurazione dopo averle apportate. Per ulteriori informazioni, consulta Implementazione delle modifiche alla configurazione. In SSM AppConfig, è necessario distribuire una nuova versione della configurazione dopo averla creata.

Disabilitazione della configurazione predefinita

È possibile disabilitare una regola di configurazione predefinita aggiungendo un blocco di configurazione con lo stesso ConfigurationID al profilo di configurazione di personalizzazione e assegnando al campo Enabled il valore false.

Ad esempio, se nel profilo di configurazione predefinito fosse presente la seguente configurazione:

```
{
 "AWS::EC2::Instance": {
  "AMSManagedBlock1": {
   "Enabled": true,
   "Filter": {
    "Platform": "Windows"
   },
   "Tags": [{
    "Key": "my-tag",
    "Value": "SampleValueA"
   }]
  }
```

```
 }
}
```

È possibile disabilitare questa regola di etichettatura includendo quanto segue nel profilo di configurazione di personalizzazione:

```
{
 "AWS::EC2::Instance": {
  "AMSManagedBlock1": {
   "Enabled": false
  }
 }
}
```

> **Important**
>
> Ricordati di implementare le modifiche alla configurazione dopo averle apportate; per informazioni, consulta. Implementazione delle modifiche alla configurazione In SSM AppConfig, è necessario distribuire una nuova versione della configurazione dopo averla creata.

Rimozione dei tag applicati da Resource Tagger

Tutti i tag con il prefisso ams:rt vengono rimossi da Resource Tagger se i tag non esistono nei profili di configurazione o, se esistono, dove il filtro non corrisponde. Ciò significa che puoi rimuovere i tag applicati da Resource Tagger effettuando una delle seguenti operazioni:

- Modifica della sezione di configurazione di personalizzazione che definisce il tag.
- Aggiungere un'eccezione per le risorse specifiche in modo che non corrispondano più al filtro.

Ad esempio: se un'istanza Linux ha i seguenti tag:

```
"Tags": [{
    "Key": "ams:rt:MyOwnTag",
    "Value": true
},{
    "Key": "myTag",
    "Value": true
```

```
}]
```

E si distribuisce il seguente profilo di configurazione Resource Tagger:

```
{
    "AWS::EC2::Instance": {
        "AMSMonitoringWindows": {
            "Enabled": true,
            "Filter": {
                "Platform": "Windows"
            },
            "Tags": [{
                "Key": "ams:rt:ams-managed",
                "Value": "true"
            }]
        }
    }
}
```

Resource Tagger reagisce alle nuove modifiche alla configurazione e l'unico tag sull'istanza diventa:

```
"Tags": [{
    "Key": "myTag",
    "Value": true
}]
```

Warning

Fai attenzione quando specifichi il nome per la tua nuova configurazione (`SampleConfigurationBlock`nell'esempio fornito) poiché potresti inavvertitamente sovrascrivere la configurazione gestita da AMS con lo stesso nome.

Important

Ricordati di distribuire le modifiche alla configurazione dopo averle apportate; per informazioni, consulta. Implementazione delle modifiche alla configurazione In SSM AppConfig, è necessario distribuire una nuova versione della configurazione dopo averla creata.

Visualizzazione o modifica della configurazione di Resource Tagger

I due profili di configurazione JSON, AMSManagedTag e CustomerManagedTags, distribuiti sul tuo account in AWS AppConfig al momento dell'onboarding e residenti nell'applicazione AMSResource Tagger e nell'AMSInfrastructureambiente, possono essere esaminati tramite l'API. AppConfig GetConfiguration

Di seguito è riportato un esempio di questa chiamata: GetConfiguration

```
aws appconfig get-configuration
 --application AMSResourceTagger
 --environment AMSInfrastructure
 --configuration AMSManagedTags
 --client-id ANY_STRING
 outfile.json
```

Applicazione: unità AppConfig logica per fornire funzionalità, per il Resource Tagger, questo è AMSResource Tagger.

- Ambiente:. AMSInfrastructure
- Configurazione: per visualizzare le definizioni dei tag predefiniti di AMS Accelerate, il valore è AMSManaged Tag, mentre per visualizzare le definizioni dei tag dei clienti, il valore è CustomerManagedTags.
- ID client: l'identificatore univoco dell'istanza dell'applicazione, può essere qualsiasi stringa.
- Le definizioni dei tag possono quindi essere visualizzate nel file di output specificato, in questo caso outfile.json.

Le definizioni degli allarmi possono quindi essere visualizzate nel file di output specificato, in questo caso outfile.json.

Puoi vedere quale versione di configurazione è stata distribuita sul tuo account visualizzando le distribuzioni precedenti nell'ambiente. AMSInfrastructure

Per sovrascrivere le regole dei tag:

Qualsiasi regola di tag esistente può essere sovrascritta aggiornando il profilo di personalizzazione con CloudFormation by Implementazione di un profilo di configurazione con CloudFormation for Accelerate o o utilizzando direttamente l'API di Using. AppConfig CreateHostedConfigurationVersion

L'utilizzo dello stesso ConfigurationID come regola del tag di configurazione predefinito sostituisce la regola predefinita e applica la regola personalizzata al suo posto.

Per distribuire le modifiche apportate al documento: CustomerManagedTags

Dopo aver apportato modifiche al profilo di configurazione di personalizzazione, è necessario distribuire le relative modifiche. Per implementare le nuove modifiche, AppConfig l'StartDeploymentAPI deve essere eseguita utilizzando la AWS AppConfig console o la CLI.

Implementazione delle modifiche alla configurazione

Una volta completata la personalizzazione, queste modifiche devono essere implementate tramite l'API. AWS AppConfig StartDeployment Le seguenti istruzioni mostrano come eseguire la distribuzione utilizzando. AWS CLI Inoltre, è possibile utilizzare il Console di gestione AWS per apportare queste modifiche. Per informazioni, consulta Fase 5: Implementazione di una configurazione.

```
aws appconfig start-deployment
--application-id <application_id>
--environment-id <environment_id>
--deployment-strategy-id <deployment_strategy_id>
--configuration-profile-id <configuration_profile_id>
--configuration-version 1
```

- ID applicazione: l'ID dell'applicazione AMSResource Tagger. Ottieni questo risultato con la chiamata ListApplicationsAPI.
- ID ambiente: l'ID dell'ambiente; ottenilo con la chiamata ListEnvironmentsAPI.
- ID della strategia di implementazione: l'ID della strategia di implementazione; ottenilo con la chiamata ListDeploymentStrategiesAPI.
- ID del profilo di configurazione: l'ID del profilo di configurazione di CustomerManagedTags; ottenilo con la chiamata ListConfigurationProfilesAPI.
- Versione di configurazione: la versione del profilo di configurazione che intendi implementare.

> **Important**
>
> Resource Tagger applica i tag come specificato nei profili di configurazione. Qualsiasi modifica manuale apportata (con o CloudWatch CLI/SDK) ai tag delle risorse viene ripristinata automaticamente, quindi assicurati che le modifiche siano definite tramite

Resource Tagger. Console di gestione AWS Per sapere quali tag vengono creati dal Resource Tagger, cerca le chiavi dei tag con il prefisso. `ams:rt:`

Limita l'accesso alla distribuzione con StartDeployment e alle azioni StopDeploymentAPI a utenti fidati che comprendono le responsabilità e le conseguenze dell'implementazione di una nuova configurazione per i tuoi obiettivi.

Per ulteriori informazioni su come utilizzare AWS AppConfig le funzionalità per creare e distribuire una configurazione, consulta la documentazione in Working with AWS AppConfig.

Configurazione di Terraform per ignorare i tag Resource Tagger

Se utilizzi Terraform per fornire le tue risorse e desideri utilizzare Resource Tagger per taggare le tue risorse, i tag Resource Tagger possono essere identificati come drift da Terraform.

Puoi configurare Terraform per ignorare tutti i tag Resource Tagger utilizzando il blocco di configurazione lifecycle o il blocco di configurazione globale ignore_tags. Per ulteriori informazioni, consulta la documentazione Terraform su Resource Tagging in Resource Tagging.

L'esempio seguente mostra come creare una configurazione globale per ignorare tutti i tag che iniziano con il prefisso del tag Resource Tagger: `ams:rt:`

```
provider "aws" {
  # ... potentially other configuration ...

  ignore_tags {
    key_prefixes = ["ams:rt:"]
  }
}
```

Visualizzazione del numero di risorse gestite da Resource Tagger

Resource Tagger invia i parametri ogni ora ad Amazon CloudWatch, nel namespace. `AMS/ResourceTagger` Le metriche vengono emesse solo per i tipi di risorse supportati da Resource Tagger.

Nome parametro	Dimensioni	Descrizione
ResourceCount	Componente, ResourceType	Numero di risorse (del tipo di risorsa specificato) distribuite in questa regione.

Nome parametro	Dimensioni	Descrizione
		Unità: numero
Resources MissingManagedTags	Componente, ResourceType	Numero di risorse (del tipo di risorsa specificato) che richiedono tag gestiti, in base ai profili di configurazione, ma non sono ancora state taggate da Resource Tagger. Unità: numero
Unmanaged Resources	Componente, ResourceType	Numero di risorse (del tipo di risorsa specificato) senza tag gestiti applicati da Resource Tagger. In genere, queste risorse non corrispondono a nessun blocco di configurazione di Resource Tagger o sono esplicitamente escluse dai blocchi di configurazione. Unità: numero
MatchingResourceCount	Componente,, ResourceType ConfigClauseName	Numero di risorse (del tipo di risorsa specificato) che corrispondono al blocco di configurazione Resource Tagger. Affinché una risorsa corrisponda al blocco di configurazione, il blocco deve essere abilitato e la risorsa deve corrispondere al filtro del blocco. Unità: numero

Queste metriche sono visualizzabili anche come grafici nella dashboard di AMS-Resource-Tagger-Reporting. Per visualizzare la dashboard, dalla console di CloudWatch gestione Amazon, seleziona AMS-Resource-Tagger-Reporting-Dashboard. Per impostazione predefinita, i grafici di questa dashboard mostrano i dati relativi al periodo precedente di 12 ore.

AMS Accelerate CloudWatch invia allarmi all'account per rilevare aumenti significativi del numero di risorse non gestite, ad esempio risorse escluse dalla gestione da AMS Resource Tagger. AMS Operations esaminerà gli aumenti delle risorse non gestite superiori a: tre risorse dello stesso

tipo o un aumento del 50% rispetto a tutte le risorse dello stesso tipo. Se la modifica non sembra intenzionale, AMS Operations potrebbe contattarti per esaminarla.

Utilizzo CloudFormation per creare tag per AMS Accelerate

Puoi utilizzarli CloudFormation per applicare i tag a livello di stack (vedi CloudFormation documentazione, tag Resource) o a livello di singola risorsa (ad esempio, vedi Tagging your Amazon EC2 resources).

> **Important**
>
> Alcuni componenti del servizio AMS Accelerate richiedono tag con il prefisso ams:rt:. Resource Tagger ritiene di possedere questi tag e li eliminerà se nessuna regola di configurazione di Resource Tagger li consente. È sempre necessario implementare un profilo di configurazione Resource Tagger per questi tag, anche se si utilizza Terraform. CloudFormation

CloudFormation Casi d'uso per AMS Accelerate

Questa sezione elenca le azioni più comuni eseguite con CloudFormation.

Argomenti

- Taggare un' EC2 istanza con CloudFormation for Accelerate
- Taggare un AutoScaling gruppo (ASG) con CloudFormation For Accelerate
- Implementazione di un profilo di configurazione con CloudFormation for Accelerate

Taggare un' EC2 istanza con CloudFormation for Accelerate

Di seguito è riportato un esempio di come è possibile applicare il tag ams:rt:ams-managed con il valore true a un'istanza Amazon gestita da. EC2 CloudFormation Il tag ams:rt:ams-managed ti consente di far monitorare le tue risorse da AMS Accelerate.

```
 Type: AWS::EC2::Instance

Properties:
  InstanceType: "t3.micro"
```

```
  # ...other properties...

  Tags:
    - Key: "ams:rt:ams-managed"
      Value: "true"
```

Taggare un AutoScaling gruppo (ASG) con CloudFormation For Accelerate

Di seguito è riportato un esempio di come è possibile applicare il tag ams:rt:ams-managed con il valore true a un gruppo Auto Scaling gestito da. CloudFormation Tieni presente che il gruppo Auto Scaling propagherà i propri tag alle EC2 istanze Amazon da esso create. Il tag ams:rt:ams-managed ti consente di far monitorare le tue risorse da AMS Accelerate.

```
  Type: AWS::AutoScaling::AutoScalingGroup
Properties:
  AutoScalingGroupName: "SampleASG"

  # ...other properties...

  Tags:
    - Key: "ams:rt:ams-managed"
      Value: "true"
```

Implementazione di un profilo di configurazione con CloudFormation for Accelerate

Se desideri distribuire il tuo profilo di `CustomerManagedTags` configurazione utilizzando CloudFormation, puoi utilizzare i seguenti CloudFormation modelli. Inserisci la configurazione JSON desiderata nel `AMSResourceTaggerConfigurationVersion.Content` campo.

Quando distribuisci i modelli in uno CloudFormation stack o in uno stack set, la distribuzione della `AMSResourceTaggerDeployment` risorsa avrà esito negativo se non hai seguito il formato JSON richiesto per la configurazione. Vedi Sintassi e struttura per i dettagli sul formato previsto.

Per assistenza sulla distribuzione di questi modelli come CloudFormation stack o set di stack, consulta la documentazione pertinente AWS CloudFormation di seguito:

- Creazione di uno stack sulla console AWS CloudFormation
- Creazione di uno stack con AWS CLI

- Creazione di un set di stack

> **Note**
>
> Se si distribuisce una versione di configurazione utilizzando uno di questi modelli e successivamente si elimina lo CloudFormation stack/stack set, la versione di configurazione del modello rimarrà la versione attualmente distribuita e non verrà effettuata alcuna distribuzione aggiuntiva. Se desideri ripristinare una configurazione predefinita, dovrai distribuire manualmente una configurazione vuota (ovvero solo{}) o aggiornare lo stack a una configurazione vuota, anziché eliminare lo stack.

JSON

```
{
  "Description": "Custom configuration for the AMS Resource Tagger.",
  "Resources": {
    "AMSResourceTaggerConfigurationVersion": {
      "Type": "AWS::AppConfig::HostedConfigurationVersion",
      "Properties": {
        "ApplicationId": {
          "Fn::ImportValue": "AMS-ResourceTagger-Configuration-ApplicationId"
        },
        "ConfigurationProfileId": {
          "Fn::ImportValue": "AMS-ResourceTagger-Configuration-CustomerManagedTags-
ProfileID"
        },
        "Content": "{\"Options\": {\"ReadOnly\": false}}",
        "ContentType": "application/json"
      }
    },
    "AMSResourceTaggerDeployment": {
      "Type": "AWS::AppConfig::Deployment",
      "Properties": {
        "ApplicationId": {
          "Fn::ImportValue": "AMS-ResourceTagger-Configuration-ApplicationId"
        },
        "ConfigurationProfileId": {
          "Fn::ImportValue": "AMS-ResourceTagger-Configuration-CustomerManagedTags-
ProfileID"
        },
```

```
        "ConfigurationVersion": {
          "Ref": "AMSResourceTaggerConfigurationVersion"
        },
        "DeploymentStrategyId": {
          "Fn::ImportValue": "AMS-ResourceTagger-Configuration-Deployment-StrategyID"
        },
        "EnvironmentId": {
          "Fn::ImportValue": "AMS-ResourceTagger-Configuration-EnvironmentId"
        }
      }
    }
  }
}
```

YAML

```
Description: Custom configuration for the AMS Resource Tagger.
Resources:
  AMSResourceTaggerConfigurationVersion:
    Type: AWS::AppConfig::HostedConfigurationVersion
    Properties:
      ApplicationId:
        !ImportValue AMS-ResourceTagger-Configuration-ApplicationId
      ConfigurationProfileId:
        !ImportValue AMS-ResourceTagger-Configuration-CustomerManagedTags-ProfileID
      Content: |
        {
          "Options": {
            "ReadOnly": false
          }
        }
      ContentType: application/json
  AMSResourceTaggerDeployment:
    Type: AWS::AppConfig::Deployment
    Properties:
      ApplicationId:
        !ImportValue AMS-ResourceTagger-Configuration-ApplicationId
      ConfigurationProfileId:
        !ImportValue AMS-ResourceTagger-Configuration-CustomerManagedTags-ProfileID
      ConfigurationVersion:
        !Ref AMSResourceTaggerConfigurationVersion
      DeploymentStrategyId:
        !ImportValue AMS-ResourceTagger-Configuration-Deployment-StrategyID
```

```
      EnvironmentId:
        !ImportValue AMS-ResourceTagger-Configuration-EnvironmentId
```

Utilizzo di Terraform per creare tag per AMS Accelerate

Se non desideri utilizzare AMS Accelerate Resource Tagger, puoi applicare i tuoi tag utilizzando Terraform. Tuttavia, se non desideri utilizzare Resource Tagger a causa della sua deriva dalle definizioni di Terraform, c'è un modo per utilizzare Resource Tagger e ignorare la deriva che causa; vedi. Configurazione di Terraform per ignorare i tag Resource Tagger

> **Important**
>
> Alcuni componenti del servizio AMS Accelerate richiedono tag con il prefisso ams:rt:. Resource Tagger ritiene di possedere questi tag e li elimina se nessuna regola di configurazione di Resource Tagger li consente. È necessario implementare un profilo di configurazione Resource Tagger per questi tag, anche se si utilizza o Terraform. CloudFormation

Di seguito è riportato un esempio di come è possibile applicare il tag ams:rt:ams-managed con il valore true a un'istanza Amazon gestita da Terraform. EC2 Il tag ams:rt:ams-managed ti consente di far monitorare le tue risorse da AMS Accelerate.

```
  resource "aws_instance" "sample_linux_instance" {
    # ...ami and other properties...

    instance_type = "t3.micro"

    tags = {
        "ams:rt:ams-managed" = "true"
    }
}
```

Di seguito è riportato un esempio di come è possibile applicare il tag ams:rt:ams-managed con il valore true a un gruppo Auto Scaling gestito da Terraform. Tieni presente che il gruppo Auto Scaling propaga i propri tag alle EC2 istanze Amazon da esso create. Il tag ams:rt:ams-managed ti consente di far monitorare le tue risorse da AMS Accelerate.

```
  resource "aws_autoscaling_group" "sample_asg" {
    # ...other properties...

    name = "terraform-sample"

    tags = {
        "ams:rt:ams-managed" = "true"
    }
}
```

Per una descrizione di come gestire i tag di risorsa creati da Terraform, consulta. Configurazione di Terraform per ignorare i tag Resource Tagger

Segnalazioni di incidenti, richieste di assistenza e domande di fatturazione in AMS Accelerate

Con AMS Accelerate, puoi richiedere assistenza per problemi e richieste operative in qualsiasi momento tramite il AWS Support Center di Console di gestione AWS. I tecnici operativi di AMS Accelerate sono disponibili per rispondere agli incidenti e alle richieste di assistenza round-the-clock, con tempi di risposta (Service Level AgreementSLAs) per il servizio. I tecnici operativi di AMS Accelerate ti informano in modo proattivo di avvisi e domande importanti utilizzando gli stessi meccanismi.

AMS Accelerate offre una gamma di servizi operativi per aiutarti a raggiungere l'eccellenza operativa su. AWS Per comprendere rapidamente come AMS aiuta i vostri team a raggiungere l'eccellenza operativa complessiva Cloud AWS grazie ad alcune delle nostre principali funzionalità operative, tra cui round-the-clock helpdesk, monitoraggio proattivo, sicurezza, applicazione di patch, registrazione e backup, consulta i diagrammi dell'architettura di riferimento di AMS.

Argomenti

- Gestione degli incidenti in AMS Accelerate
- Gestione delle richieste di assistenza in Accelerate
- Test dei report sugli incidenti e delle richieste di assistenza in Accelerate
- Domande sulla fatturazione per AMS Accelerate

Gestione degli incidenti in AMS Accelerate

In AMS Accelerate, si utilizza il AWS Support Center Consoleper archiviare i report sugli incidenti. Gli incidenti sono problemi di Servizio AWS prestazioni che influiscono sull'ambiente gestito, in base a quanto stabilito da AMS Accelerate o dall'utente. Gli incidenti identificati dal team AMS Accelerate vengono innanzitutto percepiti come eventi (una modifica dello stato del sistema rilevata dal monitoraggio). Se viene superata una soglia configurata, l'evento attiva un allarme, chiamato anche avviso. Il team operativo di AMS Accelerate determina se l'evento non ha alcun impatto, se si tratta di un incidente (interruzione o deterioramento del servizio) o se è un problema (la causa principale di uno o più incidenti).

> **Note**
>
> Il team AMS Accelerate riceve anche gli incidenti creati da te in modo programmatico utilizzando l'API AWS Support con codice di servizio. `service-ams-operations-report-incident`

Per informazioni sull'utilizzo Supporto, consulta Getting started with. Supporto

Cos'è la gestione degli incidenti?

La gestione degli incidenti è il processo utilizzato da AMS per registrare, intervenire, comunicare lo stato di avanzamento e fornire la notifica degli incidenti attivi.

L'obiettivo del processo di gestione degli incidenti è garantire che il normale funzionamento del servizio gestito venga ripristinato il più rapidamente possibile, l'impatto aziendale sia ridotto al minimo e tutte le parti interessate siano tenute informate.

Alcuni esempi di incidenti includono (ma non sono limitati a) la perdita o il deterioramento della connettività di rete, un processo o un'API che non rispondono o un'attività pianificata che non viene eseguita (ad esempio, un backup fallito).

L'immagine seguente mostra il flusso di lavoro di un incidente segnalato dall'utente ad AMS.

Questo grafico mostra il flusso di lavoro di un incidente segnalato da AMS all'utente.

Priorità dell'incidente

Gli incidenti creati nel centro di supporto AWS, nella console o nell'API Support (SAPI) hanno classificazioni diverse rispetto agli incidenti creati nella console AMS.

- Basso: le funzioni non critiche del servizio o dell'applicazione aziendale relative alle risorse AWS o AMS ne risentono.
- Medio: un servizio o un'applicazione aziendale relativi alle risorse AWS and/or AMS subisce un impatto moderato e funziona in uno stato degradato.
- Alto: la tua azienda ne risente in modo significativo. Le funzioni critiche dell'applicazione relative alle risorse AWS and/or AMS non sono disponibili. Riservato alle interruzioni più critiche che interessano i sistemi di produzione.

> **Note**
>
> La console AWS Support offre cinque livelli di priorità degli incidenti che traduciamo nei tre livelli AMS.

Come funzionano la risposta e la risoluzione degli incidenti

AMS Accelerate utilizza le migliori pratiche di gestione dei servizi IT (ITSM) per ripristinare il servizio, quando necessario, il più rapidamente possibile.

Forniamo follow-the-sun assistenza 24 ore su 24, 7 giorni su 7, 365 giorni all'anno attraverso centri operativi in tutto il mondo, con operatori dedicati che controllano attivamente i dashboard di monitoraggio e le code degli incidenti.

I nostri tecnici operativi utilizzano strumenti interni di tracciamento degli incidenti per identificare, registrare, classificare, assegnare priorità, diagnosticare, risolvere e chiudere gli incidenti; ti forniamo aggiornamenti su tutte queste attività tramite Support Center e tramite l'API AWS Support. AWS I nostri operatori si avvalgono di una varietà di strumenti di AWS supporto interni per aiutarli in tutte queste attività. Questi operatori hanno una profonda familiarità con l'infrastruttura supportata da AMS Accelerate e dispongono di competenze tecniche di livello esperto per risolvere i problemi di supporto identificati. Nel caso in cui i nostri operatori necessitino di assistenza, sono disponibili il Premium Support e i team di AWS assistenza.

Dopo che l'incidente è stato ricevuto dal team operativo di AMS Accelerate, verificheremo la priorità e la classificazione collaborando con voi per eventuali chiarimenti. Ad esempio, se la segnalazione dell'incidente è meglio classificata come richiesta di servizio, viene riclassificata e il team di richiesta di assistenza di AMS Accelerate prende il sopravvento e tu ricevi una notifica. Se l'incidente può essere risolto dall'operatore ricevente, vengono prese misure per risolverlo rapidamente. Gli operatori di AMS Accelerate consultano la documentazione interna per una risoluzione e, se necessario, inoltrano l'incidente ad altre risorse di supporto fino alla risoluzione dell'incidente. Una volta risolto, il team operativo di AMS Accelerate documenta l'incidente e la risoluzione per usi futuri.

Nei casi in cui incidenti di gravità critica influiscano sui carichi di lavoro critici, AMS Accelerate può consigliare un ripristino dell'infrastruttura. Spesso esiste un compromesso tra la risoluzione di un problema e il semplice ripristino da un backup funzionale noto, e i rischi e gli impatti derivanti dai tempi di inattività del servizio sono i fattori decisivi. Se hai tempo da dedicare alla risoluzione dei problemi, AMS Accelerate ti assisterà e il tuo cloud service delivery manager (CSDM) potrebbe

intervenire, ma se l'urgenza del ripristino è elevata, AMS Accelerate può avviare immediatamente un ripristino.

Gestione degli incidenti in AMS Accelerate

Da AWS Support Center, è possibile eseguire le seguenti attività:

- Segnalare e aggiornare un incidente. Per segnalare un incidente con AMS Accelerate, scegli AMS Operations -- Segnala incidente dal menu Servizi.
- Ottieni un elenco e informazioni dettagliate su tutti gli incidenti che hai inviato.
- Restringi la ricerca degli incidenti in base allo stato e ad altri filtri.
- Aggiungi comunicazioni e file allegati ai tuoi incidenti e aggiungi destinatari e-mail per la corrispondenza dei casi.
- Avvia una chat dal vivo o richiedi una chiamata in merito al tuo incidente.

> **Note**
>
> La funzione di chat dal vivo non è destinata agli eventi di sicurezza; per problemi di sicurezza, crea una richiesta di supporto ad alta priorità (P1 o P2).

- Risolvi gli incidenti.
- Valuta le comunicazioni relative agli incidenti.

Gli esempi seguenti descrivono l'utilizzo del Support Center per inviare un incidente. Dopo l'invio, il team di AMS Accelerate collabora con te per risolvere l'incidente in base allo SLA standard di AMS Accelerate.

Invio di un incidente per Accelerate

Per segnalare un incidente utilizzando Support Center, consulta la documentazione di supporto: Creazione di un caso di supporto

Per segnalare un incidente utilizzando Supporto center:

1. Fai clic su Crea caso. Viene visualizzata la pagina di creazione del caso di incidente.
2. Apri il menu del tipo di problema relativo al supporto tecnico e scegli AMS Operations -- Segnala incidente. Fornisci informazioni sull'incidente e scegli Crea.

3. Per essere informato via e-mail in ogni fase del processo di risoluzione degli incidenti, assicurati di compilare l'opzione CC Emails; se ti connetti tramite federazione, accedi prima di seguire il link sull'incidente contenuto nell'e-mail che AMS Accelerate ti invia.

> **Note**
>
> La descrizione dovrebbe essere quanto più dettagliata possibile e includere informazioni sulle risorse rilevanti, oltre a qualsiasi altra informazione che potrebbe esserci utile per capire il tuo problema. Ad esempio, per la risoluzione dei problemi relativi alle prestazioni, includi time stamp e log. Per la richiesta di caratteristiche o di informazioni generali, includi una descrizione dell'ambiente e dello scopo. In tutti i casi, segui le Description Guidance (Linee guida per la descrizione) visualizzate sul modulo per l'invio del caso.
> Fornendo il maggior numero di dettagli possibile, aumenti le probabilità che il tuo caso venga risolto in modo rapido.

Puoi anche utilizzare l'API AWS Support con codice di servizio `service-ams-operations-report-incident` per segnalare un incidente.

Monitoraggio e aggiornamento di un incidente Accelerate

È possibile aggiornare, monitorare ed esaminare i report sugli incidenti e le richieste di assistenza, entrambi denominati casi, utilizzando Support Center o a livello di codice utilizzando l'operazione Supporto API. `DescribeCases`

Per monitorare un caso, un incidente o una richiesta di assistenza utilizzando Supporto Center, procedi nel seguente modo.

1. Nella console AWS di gestione, accedi a Support.
2. Dal menu di navigazione a sinistra, seleziona I tuoi casi di assistenza, seleziona un caso e scegli il link Oggetto per aprire una pagina dei dettagli con lo stato attuale e le corrispondenze.

   Se a questo punto desideri utilizzare il telefono o la chat, fai clic su Apri caso in Support Center per aprire la pagina Crea caso nel Supporto Centro, compilata automaticamente con il tipo di servizio AMS.

Quando un incidente segnalato o un caso di richiesta di assistenza viene aggiornato dal team operativo di Accelerate, ricevi un'e-mail e un link all'incidente nel Support Center in modo da poter rispondere.

> **Note**
>
> Non puoi rispondere alla corrispondenza relativa al caso rispondendo all'e-mail.

Se ci sono molti casi nella dashboard, puoi utilizzare l'opzione Filtro:

- Oggetto: utilizza questo filtro per cercare parole chiave nell'oggetto del caso.
- Severità: Utilizzalo per filtrare i casi in base alla gravità selezionando una gravità dall'elenco.
- Tipo di caso: utilizza questa opzione per visualizzare tutti i casi di un particolare tipo di caso. Gli incidenti di Accelerate e le richieste di assistenza vengono visualizzati nella categoria Technical Support Case Type, insieme a tutti i casi specifici di assistenza.
- Stato: utilizza questa opzione per filtrare i casi in base allo stato selezionando uno stato specifico dall'elenco.

3. Per verificare lo stato più recente, aggiorna la pagina.
4. Se le corrispondenze sono così numerose che non vengono visualizzate tutte nella pagina, scegli Carica altro.
5. Per aggiornare lo stato del caso, scegli Rispondi, inserisci la nuova corrispondenza, quindi scegli Invia.
6. Per chiudere il caso dopo che è stato risolto in modo soddisfacente, scegli Chiudi caso.

   Assicurati di assegnare al servizio una valutazione da 1 a 5 stelle per far sapere ad AMS come stiamo.

Gestione degli incidenti Accelerate con l'API di supporto

Puoi utilizzare l'Supporto API per creare incidenti e aggiungere corrispondenza con il Supporto personale durante le indagini sui tuoi problemi. L' Supporto API modella gran parte del comportamento del AWS Support Center.

Per informazioni sull'utilizzo di questo servizio di AWS supporto, consulta Programming the Life of an AWS Support Case.

> **Note**
>
> Il team di AMS Accelerate riceve gli incidenti creati dall'utente in modo programmatico utilizzando il codice di servizio with. `service-ams-operations-report-incident`

Risposta a un incidente generato da AMS Accelerate

AMS Accelerate monitora in modo proattivo le tue risorse. Per ulteriori informazioni, consulta Monitoraggio e gestione degli eventi in AMS Accelerate. A volte AMS Accelerate identifica e crea un incidente, il più delle volte per avvisarti di un evento. Se è necessaria un'azione da parte tua per risolvere un incidente, il team di AMS Accelerate invia una notifica alle informazioni di contatto che hai fornito per l'account. Rispondi a questa notifica nello stesso modo in cui rispondi a qualsiasi altro problema, in genere tramite Support Center, sebbene in alcuni casi sia necessario il contatto tramite e-mail o telefono.

> **Important**
>
> Per ricevere notifiche di modifica dello stato per un incidente, un caso o una richiesta di assistenza, inserisci un indirizzo e-mail nel campo degli indirizzi.

Guarda il video di Akshay per saperne di più (4:15)

Gestione delle richieste di assistenza in Accelerate

Argomenti

- Quando utilizzare una richiesta di assistenza per Accelerate
- Come funziona la gestione delle richieste di assistenza in Accelerate
- Creazione di una richiesta di servizio in Accelerate
- Monitoraggio e aggiornamento di una richiesta di servizio per Accelerate
- Gestione delle richieste di assistenza con l'API di supporto per Accelerate
- Risposta a una richiesta di assistenza generata da AMS Accelerate

AMS Accelerate utilizza la gestione delle richieste di assistenza per registrare, intervenire, comunicare lo stato di avanzamento e fornire notifiche delle richieste di servizio attive.

L'obiettivo del processo di gestione delle richieste di assistenza è garantire che il servizio gestito fornisca ciò di cui hai bisogno.

Per domande relative alla fatturazione, crea una richiesta di servizio.

> **Note**
>
> Il team AMS Accelerate riceve le richieste di servizio create da te in modo programmatico utilizzando l'API AWS Support con codice di servizio. `service-ams-operations-service-request`

Utilizzando AWS Support Center, puoi eseguire le seguenti attività:

- Segnala e aggiorna una richiesta di servizio. Per una richiesta di assistenza AMS Accelerate, scegli AMS Operation -- Service Request dal menu Servizi.
- Ottieni un elenco e informazioni dettagliate su tutte le richieste di assistenza inviate.
- Restringi la ricerca delle richieste di assistenza in base allo stato e ad altri filtri.
- Aggiungi comunicazioni e file allegati alle tue richieste e aggiungi destinatari e-mail per la corrispondenza dei casi.
- Risolvi le richieste di assistenza.
- Valuta le comunicazioni relative alle richieste di assistenza.

Quando utilizzare una richiesta di assistenza per Accelerate

I seguenti esempi descrivono una richiesta di assistenza. Dopo aver inviato una richiesta di assistenza, il team AMS Accelerate collabora con te per risolvere la richiesta in base al tuo SLA AMS.

- AMS o linee AWS guida generali
- Domande relative a Patch MW
- Domande relative alla pianificazione del backup
- Domande sulla funzionalità dei AWS servizi

Di seguito sono riportati alcuni esempi di ciò che non dovrebbe essere indicato in una richiesta di servizio:

- Problemi di accesso
- Errore nella patch
- Errore di backup

Come funziona la gestione delle richieste di assistenza in Accelerate

Le richieste di assistenza vengono gestite dal team operativo AMS Accelerate disponibile su richiesta.

Dopo che la richiesta di assistenza è stata ricevuta dal team operativo di AMS Accelerate, viene esaminata per assicurarsi che sia classificata correttamente come richiesta di servizio o incidente. Se viene riclassificato come incidente, inizia il processo di gestione degli incidenti di AMS Accelerate e ti viene inviata una notifica.

Se l'operatore AMS Accelerate è in grado di risolvere la richiesta di servizio, le misure necessarie vengono prese immediatamente. Ad esempio, se la richiesta di assistenza riguarda consigli di architettura o altre informazioni, l'operatore indirizza l'utente alle risorse appropriate o risponde direttamente alla domanda.

Se l'analisi della richiesta di servizio identifica un bug o una richiesta di funzionalità, AMS invia una notifica tramite la richiesta di servizio. Poiché non esiste un ETA per le richieste di funzionalità o la correzione di bug, la richiesta di servizio originale viene chiusa. Contatta il tuo CSDM per domande di follow-up relative alla richiesta di servizio originale.

Se la richiesta di servizio non rientra nell'ambito delle operazioni di AMS Accelerate, l'operatore invia la richiesta al vostro responsabile della fornitura dei servizi cloud, in modo che possa comunicare con voi, oppure al team di AWS supporto appropriato, inviandovi un'e-mail con le informazioni sulle misure da intraprendere.

La richiesta di assistenza non viene risolta finché l'utente non ha dichiarato di essere soddisfatto del risultato.

> **Note**
>
> Ti consigliamo di fornire un indirizzo email, un nome e un numero di telefono di contatto in tutti i casi per facilitare le comunicazioni.

Creazione di una richiesta di servizio in Accelerate

Per creare una richiesta di servizio, procedi nel seguente modo:

1. Dalla console AMS Accelerate, accedi a Dashboard.
2. Scegli Apri una richiesta di assistenza, l'AMS — Service Request è preselezionato.
3. Scegli una categoria.
4. Scegli Severity (solo livelli Plus o Premium).
5. Inserisci le informazioni per:

   - Oggetto: un titolo descrittivo per la richiesta di assistenza.
   - Descrizione: una descrizione completa della richiesta di servizio, dei sistemi interessati e del risultato previsto di una risoluzione.
6. Per aggiungere un allegato, scegliete Allega file, individuate l'allegato desiderato e scegliete Apri.

   Per eliminare l'allegato, scegliete l'icona di eliminazione
7. Contattaci: il contatto predefinito AMS tramite il Web. Per selezionare altre opzioni:

   - Lingua di contatto preferita: l'inglese è la lingua supportata per le richieste di assistenza AMS Accelerate.
   - Web: la richiesta di assistenza viene inviata tramite il Web e gestita dal team operativo AMS.
   - Chat: chatta online con un rappresentante operativo di AMS Accelerate. Questa opzione ti aggiunge alla coda della chat.
   - Telefono: un rappresentante delle operazioni AMS ti richiama. Inserisci la regione AWS, il numero di telefono e l'estensione, se applicabile.
   - Contatti aggiuntivi: inserisci eventuali indirizzi email aggiuntivi che desideri vengano copiati nella richiesta di servizio.
8. Scegli Invia.

   Si apre una pagina con i dettagli del caso con informazioni sulla richiesta di assistenza, ad esempio Tipo, Oggetto, Creato, ID e Stato. Inoltre, un'area di corrispondenza che include la descrizione della richiesta creata.

   Per aprire un'area di corrispondenza e fornire ulteriori dettagli o aggiornamenti sullo stato, scegli Rispondi.

   Dopo aver risolto la richiesta di assistenza, scegli Risolvi caso.

Se le corrispondenze sono così tante che non compaiono tutte nella pagina, scegli Carica altro.

Assicurati di assegnare al servizio una valutazione da 1 a 5 stelle per far sapere ad AMS come stiamo andando.

> **Note**
>
> Se intendi testare la funzionalità della richiesta di assistenza, ti consigliamo di aggiungere un contrassegno di non intervento all'oggetto della richiesta di servizio, ad esempio. `AMSTestNoOpsActionRequired` Quindi puoi eseguire il test senza avviare il processo di risoluzione delle richieste di assistenza.
> Il team AMS Accelerate riceve le richieste di servizio create da te in modo programmatico utilizzando l'API AWS Support con codice di servizio. `service-ams-operations-service-request`

Monitoraggio e aggiornamento di una richiesta di servizio per Accelerate

Per monitorare un caso, un incidente o una richiesta di assistenza, utilizzando Supporto Center, segui questi passaggi.

1. Nella console AWS di gestione, accedi a Support.
2. Dal menu di navigazione a sinistra, seleziona I tuoi casi di assistenza, seleziona un caso e scegli il link Oggetto per aprire una pagina dei dettagli con lo stato attuale e le corrispondenze.

   Se a questo punto desideri utilizzare il telefono o la chat, fai clic su Apri caso in Support Center per aprire la pagina Crea caso nel Supporto Centro, compilata automaticamente con il tipo di servizio AMS.

   Quando un incidente segnalato o un caso di richiesta di assistenza viene aggiornato dal team operativo di Accelerate, ricevi un'e-mail e un link all'incidente nel Support Center in modo da poter rispondere.

   > **Note**
   >
   > Non puoi rispondere alla corrispondenza relativa al caso rispondendo all'e-mail.

Se ci sono molti casi nella dashboard, puoi utilizzare l'opzione Filtro:

- Oggetto: utilizza questo filtro per cercare parole chiave nell'oggetto del caso.
- Severità: Utilizzalo per filtrare i casi in base alla gravità selezionando una gravità dall'elenco.
- Tipo di caso: utilizza questa opzione per visualizzare tutti i casi di un particolare tipo di caso. Gli incidenti di Accelerate e le richieste di assistenza vengono visualizzati nella categoria Technical Support Case Type, insieme a tutti i casi specifici di assistenza.
- Stato: utilizza questa opzione per filtrare i casi in base allo stato selezionando uno stato specifico dall'elenco.

3. Per verificare lo stato più recente, aggiorna la pagina.
4. Se le corrispondenze sono così numerose che non vengono visualizzate tutte nella pagina, scegli Carica altro.
5. Per aggiornare lo stato del caso, scegli Rispondi, inserisci la nuova corrispondenza, quindi scegli Invia.
6. Per chiudere il caso dopo che è stato risolto in modo soddisfacente, scegli Chiudi caso.

   Assicurati di assegnare al servizio una valutazione da 1 a 5 stelle per far sapere ad AMS come stiamo.

Gestione delle richieste di assistenza con l'API di supporto per Accelerate

Puoi utilizzare l'API AWS Support per creare richieste di assistenza e aggiungervi corrispondenza durante le indagini sui problemi e le interazioni con il personale di AWS supporto. L'API di AWS supporto modella gran parte del comportamento del AWS Support Center.

Il team AMS riceve anche le richieste di servizio create da te a livello di codice utilizzando l'API AWS Support con il codice service-ams-operations-service di servizio -request.

Per ulteriori informazioni su come utilizzare questo servizio di AWS supporto, vedere Programming the Life of an AWS Support Case.

Risposta a una richiesta di assistenza generata da AMS Accelerate

AMS Accelerate monitora in modo proattivo le tue risorse; per ulteriori informazioni, consulta. Monitoraggio e gestione degli eventi in AMS Accelerate A volte AMS Accelerate crea una richiesta di servizio o una notifica di servizio per conto dell'utente, in genere se è necessaria un'azione da

parte dell'utente per risolvere una richiesta di servizio. In tal caso, il team di AMS Accelerate invia una notifica al contatto che hai fornito per l'account. Rispondi a questa richiesta di assistenza nello stesso modo in cui rispondi in qualsiasi altro caso, in genere tramite il Support Center, sebbene in alcuni casi sia necessaria la corrispondenza via e-mail o telefonica.

> **Important**
>
> Per ricevere notifiche di modifica dello stato per una richiesta di servizio o un caso imprevisto, è necessario aver inserito un indirizzo e-mail nel campo degli indirizzi. Le notifiche vengono inviate solo all'indirizzo e-mail aggiunto al caso al momento della creazione.

Il link contenuto nell'e-mail di notifica funziona solo se utilizzi un server di posta elettronica sulla tua rete federata AMS Accelerate. Altrimenti, puoi rispondere alla corrispondenza accedendo alla tua console AMS Accelerate e utilizzando la pagina dei dettagli del caso.

> **Note**
>
> AMS Accelerate invia le comunicazioni all'indirizzo e-mail principale del tuo AWS account; ti consigliamo di aggiungere un alias e-mail di contatto operativo alternativo per facilitare il processo di gestione del servizio request/notification . Questo è coperto durante il processo di onboarding di AMS Accelerate e nella relativa documentazione di onboarding.

Test dei report sugli incidenti e delle richieste di assistenza in Accelerate

Quando testate le segnalazioni di incidenti o le richieste di assistenza, vi chiediamo di includere AMSTestNoOpsActionRequirednell'oggetto il testo. Ciò consente ad AMS di sapere che l'incidente o la richiesta è solo a scopo di test. Quando i tecnici operativi di AMS lo vedono, non rispondono in alcun modo.

Domande sulla fatturazione per AMS Accelerate

Per inviare una domanda relativa alla fatturazione, completa i seguenti passaggi:

1. Apri il Supporto AWS Centro a casa#/ https://console.aws.amazon.com/support/.

2. Scegli Account e fatturazione.

3. Scegli Crea caso.

4. Scegli Account e fatturazione, quindi segui le istruzioni per inviare la tua richiesta.

Gestione pianificata degli eventi in AWS Managed Services

La gestione pianificata degli eventi (PEM) di AWS Managed Services (AMS) è un'offerta di servizi AMS. PEM coinvolge, coordina e assiste i clienti durante gli eventi e i progetti che utilizzano i servizi AMS. Il PEM aiuta a coordinare una serie di attività correlate in linea con l'ambito e la tempistica concordati dell'evento o del progetto PEM.

Criteri AMS PEM

Un evento pianificato è un progetto limitato a un ambito e a una scadenza. AMS utilizza i dettagli forniti dall'utente (tra cui piano e ambito, risultati attesi e modifiche che le operazioni di AMS dovrebbero eseguire) per supportarti efficacemente durante l'attività PEM. I tuoi Cloud Architects (CAs) esaminano e valutano quindi l'attività PEM per verificarne la completezza, l'implementazione tecnica e il coinvolgimento delle operazioni AMS. Dopo la revisione da parte di CA, AMS Operations esamina i piani e si coordina con il responsabile della fornitura dei servizi cloud (CSDM) per il coinvolgimento del team operativo.

Tipi di PEM

Di seguito sono riportati i tipi di PEM disponibili:

- Giorni di gioco
  - Operational Gameday: un approccio di gioco basato su scenari alla risposta operativa, volto a convalidare l'integrazione di processi, persone e sistemi.
  - Security Gameday: una strategia di risposta agli incidenti di sicurezza che utilizza un approccio di gioco basato su scenari per valutare l'integrazione di sistemi, processi e personale.
- Evento di sicurezza del cliente: eventi di sicurezza pianificati. Ad esempio, test di penetrazione.
- Supporto alla migrazione: supporto per attività di onboarding e migrazione pianificate.

Questo flusso di lavoro facilita la collaborazione con AMS per il coordinamento degli eventi pianificati e delle attività di migrazione relative al supporto AMS. Per ricevere assistenza in merito alle vostre esigenze specifiche, contattate il vostro CSDM.

Il processo AMS PEM

Il processo PEM consiste nelle seguenti fasi:

- Iniziazione PEM: collaborate con il vostro CSDM per definire l'obiettivo per l'evento pianificato e determinare ciò che serve ad AMS Operations. AMS CAs esamina gli aspetti tecnici del piano PEM. La CAs collaborazione con AMS Security and Operations sulla conformità, l'ottimizzazione dell'esecuzione e l'automazione e sulla definizione delle attività e dei risultati di esecuzione pre-PEM. Quindi, il CSDM crea il ticket PEM e fornisce ad AMS le informazioni sul progetto e i dettagli tecnici. AMS richiede un lead time di 14 giorni di calendario per consentire al team AMS Operations di pianificare, fornire la revisione tecnica e assegnare le risorse.
- Revisione PEM: il team AMS Operations esamina la richiesta PEM e collabora con il CSDM per verificare che le informazioni contenute nel piano PEM siano corrette e complete.
- Accettazione PEM: AMS esamina le informazioni fornite e comunica al CSDM quale sarà il livello di supporto durante l'attività PEM. Se il PEM contiene informazioni complete e il CSDM concorda con lo scopo del lavoro, il PEM viene approvato.
- Prontezza ed esecuzione: AMS assicura che le attività necessarie prima dell'inizio del PEM siano completate e facilita le comunicazioni interne e con i clienti. AMS si assicura che il piano PEM funzioni correttamente e fornisce report sullo stato e sull'avanzamento.

PEM FAQs

Come posso coinvolgere AMS tramite Cases: Service Request (SRs) /Incident durante un evento PEM?

- Utilizza l'ID PEM condiviso dal tuo CSDM nella riga dell' RFC/SR oggetto del formato. `PEM-ID`

  Ove applicabile, puoi utilizzare l'opzione Contatti in diretta.
- Puoi anche creare una Service Request (SR) per discutere dei tuoi casi d'uso o per domande sull'evento pianificato. Se utilizzi un SR, non è necessario che il PEM sia valido.

Quali convalide vengono eseguite quando viene presentato un caso relativo al PEM?

- Verifica che l'ID dell'account sia elencato nel PEM.
- Verifica che lo stato PEM sia approvato e attivo tra le date di inizio e fine fornite.
- Un collegamento ai dettagli PEM viene fornito internamente agli ingegneri AMS.

Esistono SLAs o sono SLOs per richieste PEM?

- PEMs non sono associati a SLAs o SLOs.

- SLAs e SLOs per quanto riguarda gli elementi di lavoro relativi al PEM (Service Request, Incidents) sono definiti da AMS. SLOs

  Per ulteriori informazioni, consulta Rapporti sugli incidenti, richieste di assistenza e domande sulla fatturazione in AMS Accelerate.

Possiamo creare un PEM tramite una Service Request (SR)?

- No, la creazione di PEM deve essere gestita dal Cloud Service Delivery Manager (CSDM).

Operazioni su richiesta

Operations on Demand (OOD) è una funzionalità di AWS Managed Services (AMS) che estende l'ambito standard del piano operativo AMS fornendo servizi operativi che attualmente non sono offerti nativamente dai piani operativi AMS o AWS. Una volta selezionata, l'offerta del catalogo viene fornita da una combinazione di automazione e risorse AMS altamente qualificate. Non sono previsti impegni a lungo termine o contratti aggiuntivi, il che consente di estendere l'AMS e AWS le operazioni e le funzionalità esistenti in base alle esigenze. L'utente accetta di acquistare blocchi di ore (blocchi OOD), 20 ore per blocco, su base mensile.

Puoi scegliere dal catalogo di offerte standardizzate e avviare un nuovo impegno OOD tramite una richiesta di servizio. Esempi di offerte OOD includono l'assistenza per la manutenzione di Amazon EKS, le operazioni e la gestione dei AWS Control Tower cluster SAP. Le nuove offerte di cataloghi vengono aggiunte regolarmente in base alla domanda e ai casi d'uso operativi che vediamo più spesso.

OOD è disponibile per i piani operativi di AMS Advanced e AMS Accelerate ed è disponibile Regioni AWSovunque sia disponibile AMS.

AMS esegue il Customer Security Risk Management (CSRM) mentre implementa le modifiche richieste. Per ulteriori informazioni sul processo CSRM, consulta Change Request Security Reviews.

Catalogo di offerte Operations on Demand

Operations on Demand (OOD) offre i servizi descritti nella tabella seguente.

> **Note**
>
> Per le definizioni dei termini chiave, consulta la documentazione di AWS Managed Services Key Terms.

Piano operativo	Titolo	Descrizione	Risultati attesi
AMS Advanced e AMS Accelere	Manutenzione dei cluster Amazon EKS	AMS libera gli sviluppatori di container gestendo la manutenzione continua delle distribuzioni di Amazon Elastic Kubernete	I team dei clienti hanno fornito assistenza nelle operazioni di base

		s Service (Amazon EKS). AMS esegue le end-to-end procedure necessarie per aggiornare un cluster occupandosi dei component i del piano di controllo, dei componenti aggiuntivi e dei nodi. AMS esegue l'aggiornamento ai tipi di nodi gestiti e a un set curato di componenti aggiuntivi Amazon EKS e Kubernetes.	relative all'aggio rnamento dei cluster Amazon EKS.
AMS Accelera	Edilizia e vendita AMI	AMS fornisce ai clienti la gestione continua degli edifici e dei distribut ori AMI. I nostri ingegneri eseguono un rilascio mensile di AMI sottoscri tte, rilasciano AMI su richiesta per attività di patching emergenti, gestiscono le modifiche utilizzando i runbook e monitorano le build AMI utilizzando Monitoring. CloudWatc h Forniamo inoltre assistenza per la risoluzione dei problemi e rapporti dettagliati per tutte le AMI utilizzat e negli account designati. Questa offerta richiede l'implementazione di AMI build Pipelines tramite EC2 Image Builder. AMS non supporta nessun'altra automazione o servizio che interagisce con EC2 Image Builder.	Il livello di sicurezza dei clienti è migliorat o e il tempo dedicato dai clienti alla costruzione e alla distribuzione è stato ridotto. AMIs

AMS Accelera	Esecuzione delle modifiche curata	Collaborate con i nostri tecnici operativi qualificati per tradurre i vostri requisiti aziendali in richieste di modifica convalidate che possono essere eseguite in sicurezza all'interno del vostro AWS ambiente. Sfruttate il nostro approccio unico all'automazione e alla conoscenza delle migliori pratiche operative (ad esempio, valutazione dell'impatto, rollback, regola delle due persone), che si tratti di un semplice cambiamen to su larga scala o di un'azione complessa con impatti a valle.	I clienti ci hanno aiutato a definire, creare ed eseguire richieste di modifica personalizzate. Le modifiche possono essere manuali o automatizzate (CloudFormation, SSM). Include la consulenza Supporto per una guida alla configurazione, se necessario. Non destinato alle modifiche al codice dell'appl icazione, all'insta llazione/distribuzione dell'applicazione, alla migrazione dei dati o alle modifiche alla configurazione del sistema operativo.

AMS Accelera	AWS Network Firewall Operazioni	AMS collabora con te per integrare il firewall e implementare e gestire le politiche e le regole per le operazioni continue del firewall. I nostri ingegneri lo fanno sfruttando le nostre migliori pratiche operative e l'automazione per configurare politiche e regole standardizzate e abilitando il monitoraggio per rilevare le modifiche apportate al di fuori del processo di automazione. AMS notifica rapidamente le modifiche indesiderate e offre opzioni per includerle, se richiesto, o ripristinare l'account a una configurazione precedente per garantire la stabilità complessiva dei sistemi.	I team dei clienti hanno contribuito a ridurre il sovraccarico di gestione rilevando rapidamente le modifiche involontarie del firewall di rete, con conseguente migliore risoluzione degli incidenti e riduzione dei tempi di analisi delle cause principali per i problemi previsti e imprevisti.
AMS Accelera	AWS Control Tower operazioni	Operazioni e gestione continue della zona di AWS Control Tower atterraggio, incluso AWS Transit Gateway e AWS Organizations fornitura di una soluzione completa per le zone di atterraggio. Gestiamo la vendita degli account, la gestione di SCP e OU, la correzione degli errori, la gestione degli utenti SSO e AWS Control Tower gli aggiornamenti con la nostra libreria di controlli e guardrail personalizzati.	I team dei clienti hanno fornito assistenza in alcune delle attività operative di base relative alla gestione AWS Control Tower di AWS Transit Gateway e AWS Organizations.

AMS Accelera	AWS landing zone Accelera le operazioni	AMS fornisce operazioni continue delle zone di AWS atterraggio utilizzate tramite AWS Landing Zone Accelerator (LZA). I nostri ingegneri gestiscono le modifiche ai file di configura zione, la gestione dell'ambiente AWS Control Tower (CT) (vendita di account, creazione di unità organizzative, guardrail CT), la gestione delle policy di controllo dei servizi (SCP), il rilevamento e la correzione delle deviazioni CT, la gestione della configurazione di rete e gli aggiornamenti a CT e al framework LZA. AWS LZA fornisce un mezzo per configurare e gestire un ambiente sicuro con più AWS account utilizzando best practice e servizi operativi come. AWS Control Tower	I team dei clienti hanno fornito assistenza nelle operazioni e nella gestione continue della soluzione AWS Landing Zone Accelerator.

AMS Accelera	SAP Cluster Assist	Allarmi, monitoraggio, applicazione di patch ai cluster, backup e risoluzione degli incidenti dedicati per i cluster SAP. Questo articolo del catalogo consente di delegare parte del lavoro operativo in corso del team operativo SAP in modo che possa concentrarsi sulla gestione della capacità e sull'ottimizzazione delle prestazioni.	I team SAP dei clienti o dei partner hanno fornito assistenza in alcune delle attività operative sottostanti. Richiede comunque al cliente di fornire altre funzionalità SAP come gestione della capacità, ottimizzazione delle prestazioni, DBA e amministrazione di base SAP.
AMS avanzato	Esecuzione RFC prioritaria	Capacità di un tecnico operativo AMS incaricato di dare priorità all'esecuzione delle richieste di modifica (RFC). Tutti gli invii ricevono un livello di risposta più elevato e l'ordine di priorità può essere modificato interagendo direttamente con gli ingegneri tramite una sala riunioni Amazon Chime.	I clienti ricevono una risposta SLO di 8 ore per. RFCs

AMS Advanced e AMS Accelere	Aggiornamento del sistema operativo legacy	Evita la migrazione delle istanze aggiornando le istanze a una versione del sistema operativo supportata. Possiamo eseguire un aggiornamento sul posto sulle istanze selezionate sfruttando l'automazione e le funzionalità di aggiornamento dei fornitori di software (ad esempio, da Microsoft Windows 2008 R2 a Microsoft Windows 2012 R2). Questo approccio è ideale per le applicazioni legacy che non possono essere facilmente reinstallate su una nuova istanza e offre una protezione aggiuntiva dalle minacce alla sicurezza note e non mitigate sulle versioni precedenti del sistema operativo. I seguenti sistemi operativi sono supportati per gli aggiornamenti in loco: • Da Microsoft Windows 2012 R2 a Microsoft Windows 2016 e versioni successive • Da Microsoft Windows 2016 a Microsoft Windows 2022 e versioni successive • Da Red Hat Enterprise Linux 7 a Red Hat Enterprise Linux 8 • Da Red Hat Enterprise Linux 8 a Red Hat Enterprise Linux 9 • Da Oracle Linux 7 a Oracle Linux 8	Questa soluzione viene fornita per le applicazioni che non possono più essere reinstallate su una nuova istanza (ad esempio, perdita del codice sorgente, ISV fuori servizio e così via). È possibile ripristinare lo stato originale degli aggiornamenti non riusciti. Dal punto di vista operativo, il rollback è preferibile perché pone l'istanza in uno stato più supportabile con le patch di sicurezza più recenti.

Argomenti

- Richiedere AMS Operations On Demand
- Apportare modifiche alle offerte Operations on Demand

Richiedere AMS Operations On Demand

AWS Managed Services (AMS) Operations on Demand (OOD) è disponibile per tutti Account AWS coloro che sono stati inseriti in AMS. Per sfruttare Operations on Demand, richiedi ulteriori informazioni al tuo cloud service delivery manager (CSDM), Solutions Architect (SA), account manager o Cloud Architect (CA). Le offerte OOD disponibili sono elencate nella precedente tabella delle offerte del catalogo di Operations on Demand. Dopo aver completato l'ambito del coinvolgimento, invia una richiesta di servizio ad AMS Operations per avviare un incarico per OOD.

Ogni richiesta di servizio OOD deve contenere le seguenti informazioni dettagliate relative all'incarico:

- Le offerte OOD specifiche richieste e per ogni offerta OOD specifica:
  - Il numero di blocchi (un blocco equivale a 20 ore di risorse operative in un determinato mese di calendario, da addebitare alla tariffa standard in vigore in quel momento per l'offerta Operations on Demand applicabile) da allocare alla specifica offerta OOD. AWS
  - L'ID dell'account per ogni account AWS Managed Services per il quale viene richiesta l'offerta OOD specifica.

Le richieste di servizio OOD devono essere inviate dall'utente tramite:

- L'account AWS Managed Services che riceve le offerte Operations on Demand applicabili, oppure
- Un account AWS Managed Services che è un account di AWS Organizations gestione in modalità con tutte le funzionalità, per conto di qualsiasi account membro che sia un account AWS Managed Services.

Dopo aver ricevuto la richiesta di servizio OOD, AMS Operations esamina e aggiorna gli account con la loro approvazione, approvazione parziale o rifiuto.

Una volta approvata la richiesta di servizio dell'offerta OOD, tu e AMS vi coordinate per iniziare l'incarico. Nessuna offerta OOD viene avviata finché la richiesta di servizio non viene approvata e non viene concordata una data di inizio dell'incarico.

AMS utilizza un'assegnazione mensile di blocchi OOD in abbonamento. Assegniamo il numero di blocchi approvato mensilmente, a partire dalla data di inizio dell'impegno, fino a quando non richiedi di rinunciare tramite una nuova richiesta di servizio. I blocchi OOD sono validi per un mese solare. I blocchi, o porzioni di blocchi, non vengono ribaltati o riportati ai mesi futuri.

Ti viene fatturato almeno un blocco OOD ogni mese, indipendentemente dal numero di ore effettivamente utilizzate. Qualsiasi blocco OOD aggiuntivo allocato in cui non sono state utilizzate ore non viene fatturato.

Apportare modifiche alle offerte Operations on Demand

Per richiedere modifiche agli impegni in corso per le offerte Operations on Demand (OOD), invia una richiesta di servizio contenente le seguenti informazioni:

- Le modifiche richieste e
- La data richiesta per l'entrata in vigore delle modifiche.

Dopo aver ricevuto la richiesta di servizio OOD, AMS Operations la esamina e la aggiorna con la propria approvazione oppure richiede che il CSDM assegnato collabori con voi per determinare l'ambito e le implicazioni della modifica. Se si ritiene che la modifica richieda uno sforzo di definizione dell'ambito da parte del CSDM, è necessario inviare una seconda richiesta di servizio OOD per avviare l'intervento modificato dopo il completamento dell'esercizio di definizione dell'ambito.

Una volta approvata, l'allocazione di blocchi modificata più di recente diventa e continua a rimanere attiva, sostituendo qualsiasi allocazione di blocchi precedente, salvo diverso accordo tra l'utente e l'utente. AWS

Rapporti e opzioni

AWS Managed Services (AMS) raccoglie dati da vari servizi AWS nativi per fornire report a valore aggiunto sulle principali offerte AMS.

AMS offre due tipi di report dettagliati:

- Report su richiesta: puoi richiedere determinati report ad hoc tramite il tuo Cloud Service Delivery Manager (CSDM). Questi report non hanno limiti perché potrebbe essere necessario richiederli più volte durante l'onboarding o gli eventi critici. Tuttavia, tieni presente che questi report non sono progettati per essere forniti secondo una pianificazione come i report settimanali. Per comprendere meglio le tue esigenze o per ulteriori informazioni sull'utilizzo dei report self-service, contatta il tuo CSDM.
- Report self-service: i report self-service AMS ti consentono di interrogare e analizzare direttamente i dati tutte le volte che ne hai bisogno. Utilizza i report self-service per accedere ai report dalla console AMS e ai set di dati di report tramite bucket S3 (un bucket per account). Ciò ti consente di integrare i dati nel tuo strumento di Business Intelligence (BI) preferito in modo da poter personalizzare i report in base alle tue esigenze.

Argomenti

- Report su richiesta
- Report self-service

Report su richiesta

Argomenti

- Rapporti sulla gestione degli host AMS
- Report di AMS Backup
- AWS Config Rapporto di controllo della conformità
- Rapporto sulla configurazione delle risposte delle regole di configurazione di AMS Config
- Incidenti evitati e monitoraggio dei report di Top Talker
- Rapporto sui dettagli degli addebiti di fatturazione
- Report di Trusted Remediator

AMS raccoglie dati da vari servizi AWS nativi per fornire report a valore aggiunto sulle principali offerte AMS. Per una copia di questi report, invia una richiesta al tuo Cloud Service Delivery Manager (CSDM).

Rapporti sulla gestione degli host AMS

Rapporti disponibili

- Rapporto sulla copertura degli agenti SSM

Rapporto sulla copertura degli agenti SSM

Il rapporto AMS SSM Agent Coverage ti informa se l'agente SSM è installato o meno nelle EC2 istanze dell'account.

Nome del campo	Definizione
Nome del cliente	Nome del cliente per situazioni in cui vi sono più clienti secondari
Regione delle risorse	AWS Regione in cui si trova la risorsa
Account name (Nome account)	Il nome dell'account
AWS ID dell'account	L'ID dell' AWS account
ID della risorsa	ID dell' EC2 istanza
Nome risorsa	Nome dell' EC2 istanza
Bandiera conforme	Indica se sulla risorsa è installato l'agente SSM («Compliant») o meno («NON_COMPLIANT»)

Report di AMS Backup

Report disponibili

- Rapporto Backup Job Success/Failure
- Rapporto di riepilogo del backup

- Summary/Coverage Rapporto di Backup

Rapporto Backup Job Success/Failure

Il Success/Failure rapporto Backup Job fornisce informazioni sui backup eseguiti nelle ultime settimane. Per personalizzare il rapporto, specifica il numero di settimane per cui desideri recuperare i dati. Il numero predefinito di settimane è 12. La tabella seguente elenca i dati inclusi nel rapporto:

Nome del campo	Definizione
ID account AWS	ID dell'account AWS a cui appartiene la risorsa
Nome dell'account	Nome dell'account AWS
ID Job di Backup	L'ID del job di Backup
ID risorsa	L'ID della risorsa di cui è stato eseguito il backup
Tipo di risorsa	Il tipo di risorsa di cui viene eseguito il backup
Regione delle risorse	La AWS regione della risorsa di cui è stato eseguito il backup
Stato di Backup	Lo stato del backup. Per ulteriori informazioni, vedere Stati dei job di Backup
ID del punto di ripristino	L'identificatore univoco del punto di ripristino
Messaggio di stato	Descrizione degli errori o degli avvisi che si sono verificati durante il processo di backup
Dimensioni del backup	Dimensioni del backup in GB
ARN del punto di ripristino	L'ARN del backup creato
Durata del punto di ripristino in giorni	Numero di giorni trascorsi dalla creazione del punto di ripristino

Nome del campo	Definizione
Meno di 30 giorni	Indicatore dei backup che risalgono a meno di 30 giorni

Rapporto di riepilogo del backup

Nome del campo	Definizione
Nome del cliente	Nome del cliente per le situazioni in cui sono presenti più clienti secondari
Mese di backup	Mese del backup
Anno di Backup	Anno del backup
Tipo di risorsa	Il tipo di risorsa di cui viene eseguito il backup
Numero di risorse	Il numero di risorse di cui è stato eseguito il backup
Numero di punti di ripristino	Numero di istantanee distinte
Backup risalenti a meno di 30 giorni	Numero di backup che risalgono a meno di 30 giorni
Età massima dei punti di ripristino	L'età più vecchia del punto di ripristino (in giorni)
Pagina minima dei punti di ripristino	Età del punto di ripristino più recente, espressa in giorni

Summary/Coverage Rapporto di Backup

Il Summary/Coverage rapporto di Backup elenca quante risorse non sono attualmente protette da alcun AWS Backup piano. Discutete con il vostro CDSM un piano appropriato per aumentare la copertura, ove possibile, e ridurre il rischio di perdita dei dati.

Nome del campo	Definizione
Nome del cliente	Nome del cliente per le situazioni in cui sono presenti più clienti secondari
Regione	AWS regione in cui si trova la risorsa
Account name (Nome account)	Il nome dell'account
AWS ID dell'account	L'ID dell' AWS account
Tipo di risorsa	Il tipo di risorsa. Le risorse sono supportat e da AWS Backup (Aurora, DocumentDB, DynamoDB, EBS, EFS EC2, RDS e S3) FSx
ARN risorsa	ARN della risorsa
ID risorsa	ID della risorsa
Copertura	Indica se la risorsa è coperta o meno («COVERED» o «NOT_COVERED»)
Numero di risorse	Numero di risorse supportate nell'account
perc_coverage	Percentuale di risorse supportate con un backup eseguito negli ultimi 30 giorni.

AWS Config Rapporto di controllo della conformità

Il rapporto AWS Config Control Compliance fornisce uno sguardo approfondito sulla conformità delle risorse e delle AWS Config regole degli account AMS. Filtra il rapporto per Config Rule Severity per dare priorità ai risultati più critici. La tabella seguente elenca i dati forniti da questo rapporto:

Campo	Descrizione
Data	Data del rapporto
Nome cliente	Nome cliente

Campo	Descrizione
AWS ID dell'account	ID AWS account associato per il cliente
Identificatore di origine	AWS Config identificatore di origine univoco della regola
Descrizione della regola	AWS Config descrizione della regola
Tipo di regola	AWS Config tipo di regola
Indicatore di conformità	AWS Config stato di conformità alle regole
Tipo di risorsa	AWS tipo di risorsa
Nome risorsa	AWS nome della risorsa
Gravità	Severità consigliata predefinita definita da AMS per la AWS Config regola
Categoria di riparazione	Categoria di risposta correttiva associata a una regola AWS Config
Descrizione della riparazione	Spiegazione delle azioni correttive per rendere la AWS Config regola conforme
Azione dell'utente	È necessaria un'azione del cliente per rendere la AWS Config regola conforme
Rapporto sulle metriche Delta	Modifiche per la conformità di una regola tra 2 date specificate

Rapporto sulla configurazione delle risposte delle regole di configurazione di AMS Config

Il rapporto AMS Config Rules Response Configuration fornisce uno sguardo approfondito su come Accelerate è attualmente configurato per rispondere a regole di configurazione AMS non conformi. Per ulteriori informazioni su come modificare la risposta per le regole di configurazione AMS, consulta AMS Accelerate Customized findings response.

Questo rapporto mostra solo le configurazioni modificate ed esclude le configurazioni predefinite di AMS elencate nella libreria delle regole di AMS Config. Il rapporto fornisce dati sulla configurazione delle risorse e sulla risposta alle regole di configurazione AMS degli account AMS, tra cui:

- L'elenco degli AWS account per i quali è stata modificata la risposta predefinita per le regole di configurazione AMS.
- L'elenco dei tag a cui hai associato una risposta per le regole di configurazione AMS.
- L'elenco delle configurazioni di risposta per ogni regola, account e tag.
- L'elenco delle risorse per le quali è stata modificata la risposta predefinita per le regole di configurazione AMS.

Rapporto sulle configurazioni di risposta più recente

Campo	Descrizione
Data	Data in cui è stato generato il rapporto
Nome cliente	Nome cliente
AWS ID dell'account	L'ID AWS dell'account associato alla configura zione
Nome dell'account	AWS nome dell'account del gruppo di risorse a livello di account
Tipo di ricerca	Tipo di reperto identificato. In questo caso, AWS Config
Identificatore di origine	AWS Config Identificatore di origine univoco della regola
ID del gruppo di risorse	L'ID del gruppo di risorse associato alla configurazione della risposta
Azione di risposta configurata	Tipo di azione attivato da AMS
SSM Runbook associato	L'eventuale Remediation Runbook che verrà eseguito

Campo	Descrizione
Tipo di gruppo di risorse	Può essere Account o Tag

Risorse con risposta predefinita personalizzata delle regole di Config

Nome del campo	Definizione
Nome cliente	Nome cliente
Data	Data in cui è stato generato il rapporto
AWS Nome dell'account	AWS nome dell'account
ID account	ID AWS dell'account associato
Regola di configurazione AMS	Regola di configurazione AMS che si rivolge alla risorsa e si applica a una configurazione
Resource ID (ID risorsa)	L'ID della risorsa nell'account del cliente oggetto della regola di configurazione AMS
Regione delle risorse	La AWS regione in cui viene applicata la configurazione
Tipo di risorsa	AWS tipo di risorsa
ID del gruppo di risorse	L'ID del gruppo di risorse associato alla configurazione della risposta
Bandiera AMS della risorsa	Se la AWS risorsa viene distribuita da AMS, questo campo è impostato su `True`
Tipo di trigger	Il tipo di risposta configurato per la risorsa
Indicatore di conformità	Stato di conformità alle regole di configurazione AMS

Incidenti evitati e monitoraggio dei report di Top Talker

Rapporti disponibili

- Rapporto sugli incidenti evitati
- Rapporto Monitoring Top Talkers

Rapporto sugli incidenti evitati

Il rapporto Incidents Prevented elenca gli CloudWatch allarmi Amazon a cui è stato posto automaticamente rimedio, prevenendo un possibile incidente. Per ulteriori informazioni, consulta Riparazione automatica. La tabella seguente elenca le informazioni incluse in questo rapporto:

Nome del campo	Definizione
execution_start_time_utc	Data in cui è stata eseguita l'automazione
nome_cliente	Nome del cliente dell'account
account_name	Il nome dell'account
AwsAccountId	L'ID dell'account AWS
nome_documento	Il nome del documento SSM o dell'automazione eseguita
durata_in_minuti	La durata dell'automazione in minuti
Regione	AWS Regione in cui si trova la risorsa
automation_execution_id	L'ID dell'esecuzione
automation_execution_status	Lo stato dell'esecuzione

Rapporto Monitoring Top Talkers

Il rapporto Monitoring Top Talkers presenta il numero di CloudWatch avvisi Amazon generati in un periodo di tempo specifico e fornisce visualizzazioni delle risorse che generano il maggior numero di avvisi. Questo rapporto ti aiuta a identificare le risorse che generano il maggior numero di avvisi.

Queste risorse potrebbero essere idonee per eseguire l'analisi della causa principale per risolvere il problema o per modificare le soglie di allarme per evitare attivazioni non necessarie quando non esiste un problema effettivo. La tabella seguente elenca le informazioni incluse in questo rapporto:

Nome del campo	Definizione
Nome cliente	Nome del cliente
AccountId	L'ID dell' AWS account
Categoria di avviso	Il tipo di avviso attivato
Descrizione	Descrizione dell'avviso
ID risorsa	ID della risorsa che ha attivato l'avviso
Nome risorsa	Nome della risorsa che ha attivato l'avviso
Regione	AWS Regione in cui si trova la risorsa
Stato dell'incidente	Stato più recente dell'incidente generato dall'allarme
Prima occorrenza	Prima volta che l'avviso è stato attivato
Evento recente	L'ultima volta in cui è stato attivato l'avviso
Numero di avvisi	Numero di avvisi generati tra la prima e la recente occorrenza

Rapporto sui dettagli degli addebiti di fatturazione

Il rapporto AWS Managed Services (AMS) Billing Charges Details fornisce dettagli sui costi di fatturazione AMS con account collegati e i rispettivi servizi AWS, tra cui:

- Costi a livello di servizio AMS, percentuali di uplift, livelli di servizio AMS a livello di account e tariffe AMS.
- Account e costi AWS di utilizzo collegati

Nome del campo	Definizione
Mese di fatturazione	Il mese e l'anno del servizio fatturato
ID del conto di pagamento	L'ID a 12 cifre che identifica l'account che sarà responsabile del pagamento degli addebiti AMS
ID dell'account collegato	L'ID a 12 cifre che identifica l'account AMS che utilizza i servizi che generano spese
AWS Nome del servizio	Il AWS servizio che è stato utilizzato
AWS Addebiti	I AWS costi per il nome del AWS servizio elencati in AWS Service Name
Piano tariffario	Il nome del piano tariffario associato all'account collegato
Proporzione di rialzo	La percentuale di aggiornamento (come V.WXYZ decimale) basata su pricing_plan, SLA e servizio AWS
Costi AWS adeguati	AWS utilizzo adattato per AMS
Costi AWS aumentati	La percentuale di addebiti AWS da addebitar e per AMS; adjusted_aws_charges * uplift_pe rcent
Istanze RDS Spend EC2	Istanze Spend on EC2 e RDS
Addebiti AMS	Costi AMS totali per il prodotto; uplifted_ aws_charges + instance_ec2_rds_spend + uplifted_ris + uplifted_sp
Tariffa minima ripartita proporzionalmente	L'importo che addebitiamo per soddisfare il minimo contrattuale
Tariffa minima	Commissioni minime AMS (se applicabile)
Costi totali AMS dell'account collegato	Somma di tutti gli addebiti per il linked_account

Nome del campo	Definizione
Costi totali AMS del conto di pagamento	Somma di tutti gli addebiti relativi al conto del pagatore

Report di Trusted Remediator

Rapporti disponibili

- Rapporto riepilogativo di Trusted Remediator Remediation
- Rapporto di riepilogo sulla configurazione di Trusted Remedi
- Trusted Advisor Controlla il rapporto di riepilogo

Rapporto riepilogativo di Trusted Remediator Remediation

Il rapporto sullo stato di Trusted Remediator Remediation fornisce informazioni sulle riparazioni avvenute durante i cicli di riparazione precedenti. Il numero predefinito di settimane è 1. Per personalizzare il rapporto, specifica il numero di settimane in base al programma di riparazione.

Nome del campo	Definizione
Data	La data in cui i dati sono stati raccolti.
ID account	L'ID AWS dell'account a cui appartiene la risorsa
Nome dell'account	Il nome AWS dell'account
Controlla la categoria	La categoria di AWS Trusted Advisor controllo
Controlla il nome	Il nome del controllo corretto Trusted Advisor
ID di controllo	L'ID del controllo corretto Trusted Advisor
Modalità di esecuzione	La modalità di esecuzione configurata per il Trusted Advisor controllo specifico

Nome del campo	Definizione
OpsItem ID	L'ID del codice OpsItem creato da Trusted Advisor per la riparazione
OpsItem Stato	Lo stato del codice OpsItem creato Trusted Advisor al momento della segnalazione
ID risorsa	L'ARN della risorsa creata per la riparazione

Rapporto di riepilogo sulla configurazione di Trusted Remedi

Il rapporto di riepilogo della configurazione di Trusted Remediator fornisce informazioni sulle configurazioni correnti di Trusted Remediator Remediation per ogni controllo. Trusted Advisor

Nome del campo	Definizione
Data	La data in cui i dati sono stati raccolti.
ID account	L'ID AWS dell'account a cui si applica la configurazione
Nome dell'account	Il nome AWS dell'account
Controlla la categoria	La categoria di AWS Trusted Advisor controllo
Controlla il nome	Il nome del Trusted Advisor controllo corretto a cui si applica la configurazione
ID di controllo	L'ID del Trusted Advisor controllo corretto a cui si applica la configurazione
Modalità di esecuzione	La modalità di esecuzione configurata per il Trusted Advisor controllo specifico
Passa a Automated	Lo schema di tag, se configurato, per sostituire la modalità di esecuzione su Automated

Nome del campo	Definizione
Sovrascrivi a Manuale	Lo schema di tag, se configurato, per sostituir e la modalità di esecuzione impostandola su Manuale

Trusted Advisor Controlla il rapporto di riepilogo

Il rapporto Trusted Advisor Check Summary fornisce informazioni sui Trusted Advisor controlli correnti. Questo rapporto raccoglie i dati dopo ogni programma di riparazione settimanale. Il numero predefinito di settimane è 1. Per personalizzare il rapporto, specifica il numero di settimane in base al ciclo di riparazione.

Nome del campo	Definizione
Data	La data in cui i dati sono stati raccolti.
ID account	L'ID AWS dell'account a cui si applica la configurazione
Nome del cliente	Il nome AWS dell'account
Controlla la categoria	La categoria di AWS Trusted Advisor controllo
Controlla il nome	Il nome del Trusted Advisor controllo corretto a cui si applica la configurazione
ID di controllo	L'ID del Trusted Advisor controllo corretto a cui si applica la configurazione
Stato	Lo stato di avviso del controllo. Gli stati possibili sono ok (verde), warning (giallo), error (rosso) o not_available
Risorse contrassegnate	Il numero di AWS risorse che sono state contrassegnate (elencate) dal controllo. Trusted Advisor

Nome del campo	Definizione
Risorse ignorate	Il numero di AWS risorse che sono state ignorate Trusted Advisor perché le hai contrassegnate come soppresse.
Risorse in stato critico	Il numero di risorse in stato critico
Risorse in stato di allerta	Il numero di risorse in stato di avviso

Report self-service

I report self-service (SSR) di AWS Managed Services (AMS) sono una funzionalità che raccoglie dati da vari AWS servizi nativi e fornisce l'accesso ai report sulle principali offerte AMS. SSR fornisce informazioni che puoi utilizzare per supportare operazioni, gestione della configurazione, gestione degli asset, gestione della sicurezza e conformità.

Usa SSR per accedere ai report dalla console AMS e ai set di dati dei report tramite i bucket Amazon S3 (un bucket per account). Puoi collegare i dati al tuo strumento di business intelligence (BI) preferito per personalizzare i report in base alle tue esigenze specifiche. AMS crea questo bucket S3 (nome del bucket S3: (ams-reporting-data-a<Account_ID>) nella AWS regione principale e i dati vengono condivisi dal piano di controllo AMS ospitato nella regione us-east-1.

Per consentire ai tuoi utenti di visualizzare i report di AMS Accelerate nella console AMS, devi concedere autorizzazioni esplicite in AWS Identity and Access Management (IAM) per eseguire tali azioni. Ad esempio, le politiche IAM, consulta Autorizzazioni all'uso delle funzionalità AMS.

Important

Utilizzo di chiavi personalizzate con AWS Glue
Per crittografare i AWS Glue metadati con una chiave KMS gestita dal cliente, è necessario eseguire i seguenti passaggi aggiuntivi per consentire ad AMS di aggregare i dati dall'account:

1. Apri la AWS Key Management Service console in https://console.aws.amazon.com/kms, quindi scegli Customer Managed Keys.
2. Seleziona l'ID della chiave che intendi utilizzare per crittografare i metadati. AWS Glue
3. Scegli la scheda Alias, quindi scegli Crea alias.

4. Nella casella di testo, immettete AmsReportingFlywheelCustomKey, quindi scegliete Crea alias.

Argomenti

- Operazioni API interne
- Rapporto sulle patch (giornaliero)
- Rapporto di Backup (giornaliero)
- Rapporto sull'incidente (settimanale)
- Rapporto di fatturazione (mensile)
- Rapporti aggregati
- Dashboard di report self-service AMS
- Policy di conservazione dei dati
- Fuori bordo da SSR

Operazioni API interne

Se monitorate le operazioni delle API, potreste vedere chiamate alle seguenti operazioni solo interne:

- `GetDashboardUrl`
- `ListReportsV2`

Funzionamento interno dell'API: GetDashboardUrl

Questa operazione appare nei log di sistema quando viene richiamata dalla console AMS. Non ha altri casi d'uso. Non è disponibile per l'uso diretto.

Restituisce l'URL della dashboard incorporata per il rapporto corrispondente. Questa operazione accetta un valore `dashboardName` restituito da`ListReports`.

Sintassi della richiesta

```
HTTP/1.1 200
Content-type: application/json
{
    "dashboardName": "string"
```

```
}
```

Elementi della richiesta

`dashboardName`: il nome della dashboard rapida per la quale viene richiesto l'URL. Il nome del dashboard viene restituito nella ListReports versione 2.

Tipo: String

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json
{
  "url": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200. I dati seguenti vengono restituiti in formato JSON mediante il servizio.

`url`: restituisce l'URL rapido per la richiesta. `dashboardName`

Tipo: String

Errori

Per informazioni sugli errori comuni a tutte le azioni, consulta Errori comuni.

`BadRequestException`:

La richiesta inviata non è valida. Ad esempio, se l'input è incompleto o errato. Per i dettagli, consulta il messaggio di errore allegato.

Codice di stato HTTP: 400

`NotFoundException`:

La risorsa richiesta non è stata trovata. Assicurati che l'URI della richiesta sia corretto.

Codice di stato HTTP: 404

`TooManyRequestsException`:

La richiesta ha raggiunto il limite di limitazione. Riprova dopo il periodo di tempo specificato.

Codice di stato HTTP: 429

`UnauthorizedException`:

La richiesta viene rifiutata perché il chiamante non dispone di autorizzazioni sufficienti.

Codice di stato HTTP: 401

Funzionamento dell'API interna: ListReports V2

Questa API appare nei log di sistema quando viene richiamata dalla console AMS. Non ha altri casi d'uso. Non è disponibile per l'uso diretto.

Restituisce un elenco di report operativi disponibili per un account specifico.

Sintassi della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json
{
  "reportsList": [
    {
        "dashboard": "string",
        "lastUpdatedTime": "string",
    }
  ],
  "reportsType": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200. I dati seguenti vengono restituiti in formato JSON mediante il servizio.

`reportsList`: L'elenco dei report operativi disponibili.

Tipo: matrice di oggetti del dashboard

`reportsType`: Indica se un rapporto è aggregato su più account o meno.

Tipo: String

Errori

Per informazioni sugli errori comuni a tutte le azioni, consulta Errori comuni.

`BadRequestException`:

La richiesta inviata non è valida. Ad esempio, l'input è incompleto o errato. Per i dettagli, consulta il messaggio di errore allegato.

Codice di stato HTTP: 400

`NotFoundException`:

La risorsa richiesta non è stata trovata. Assicurati che l'URI della richiesta sia corretto.

Codice di stato HTTP: 404

`TooManyRequestsException`:

La richiesta ha raggiunto il limite di limitazione. Riprova dopo il periodo di tempo specificato.

Codice di stato HTTP: 429

`UnauthorizedException`:

La richiesta viene rifiutata perché il chiamante non dispone di autorizzazioni sufficienti.

Codice di stato HTTP: 401

Rapporto sulle patch (giornaliero)

Report disponibili

- Riepilogo dei dettagli dell'istanza per l'applicazione delle patch ad AM
- Dettagli della patch
- Istanze in cui non sono state apportate le patch

Riepilogo dei dettagli dell'istanza per l'applicazione delle patch ad AM

Si tratta di un rapporto informativo che aiuta a identificare tutte le istanze inserite in AMS Patching, lo stato dell'account, i dettagli dell'istanza, la copertura della finestra di manutenzione, il tempo di esecuzione della finestra di manutenzione, i dettagli dello stack e il tipo di piattaforma.

Questo set di dati fornisce:

- Dati sulle istanze di produzione e non di produzione di un account. Le fasi di produzione e non produzione derivano dal nome dell'account e non dai tag dell'istanza.
- Dati sulla distribuzione delle istanze per tipo di piattaforma. Il tipo di piattaforma 'N/A' si verifica quando AWS Systems Manager (SSM) non è in grado di ottenere le informazioni sulla piattaforma.
- Dati sulla distribuzione dello stato delle istanze, sul numero di istanze in esecuzione, interrotte o terminate.

Nome del campo della console	Nome del campo del set di dati	Definizione
Restrizioni di accesso	restrizioni di accesso	Regioni a cui l'accesso è limitato
ID dell'account	aws_account_id	AWS ID dell'account a cui appartiene l'ID dell'istanza
ID dell'account di amministr atore	aws_admin_account_id	Account affidabile abilitato da te. AWS Organizations
Nome dell'account	account_name	AWS nome dell'account
Stato dell'account	account_status	stato dell'account AMS
	account_sla	Impegno al servizio dell'acco unt AMS
Tipo di account	malz_role	ruolo MALZ
Nome del gruppo con scalabili tà automatica	nome_istanza	Nome dell'Auto Scaling Group (ASG) che contiene l'istanza
ID dell'istanza	instance_id	ID dell' EC2 istanza
Nome dell'istanza	nome_istanza	Nome dell'istanza EC2
Instance Patch Group	instance_patch_group	Nome del gruppo di patch utilizzato per raggruppare le

Nome del campo della console	Nome del campo del set di dati	Definizione
		istanze e applicare la stessa finestra di manutenzione
Tipo di gruppo di patch di istanze	instance_patch_group_type	Tipo di gruppo di patch
Tipo di piattaforma di istanza	instance_platform_type	Tipo di sistema operativo (OS)
Nome della piattaforma dell'istanza	instance_platform_name	Nome del sistema operativo (OS)
Stato dell'istanza	instance_state	Stato all'interno del ciclo di vita dell'istanza EC2
Tag di istanza	ec2_tags	I tag associati all'ID dell' EC2 istanza Amazon
Zona di atterraggio	malz_flag	Contrassegna l'account relativo a MALZ
Copertura della finestra di manutenzione	mw_covered_flag	Se un'istanza ha almeno una finestra di manutenzione abilitata con date di esecuzion e future, viene considerata coperta, altrimenti non coperta
Data e ora di esecuzione della finestra di manutenzione	time_window_execution_time	La prossima volta è prevista l'esecuzione della finestra di manutenzione
Data e ora di esecuzione della finestra di manutenzione	time_window_execution_time	La prossima volta è prevista l'esecuzione della finestra di manutenzione

Nome del campo della console	Nome del campo del set di dati	Definizione
Account di produzione	prod_account	Identificatore degli account AMS prod e non prod, a seconda che il nome dell'acco unt includa o meno il valore «PROD», «NONPROD».
Data/ora del rapporto	dataset_datetime	La data e l'ora di generazione del report.
Nome stack	instance_stack_name	Nome dello stack che contiene l'istanza
Tipo di pila	instance_stack_type	Stack AMS (infrastruttura AMS all'interno dell'account del cliente) o Customer stack (infrastruttura gestita da AMS che supporta le applicazioni dei clienti)

Dettagli della patch

Questo rapporto fornisce i dettagli delle patch e la copertura della finestra di manutenzione di varie istanze.

Questo rapporto fornisce:

- Dati sui gruppi di patch e sui relativi tipi.
- Dati sulle finestre di manutenzione, durata, termine ultimo, date future di esecuzione della finestra di manutenzione (pianificazione) e istanze interessate da ciascuna finestra.
- Dati su tutti i sistemi operativi dell'account e numero di istanze in cui il sistema operativo è installato.

Nome del campo	Nome del campo del set di dati	Definizione
Data/ora del rapporto	dataset_datetime	La data e l'ora di generazione del report.
ID dell'account	aws_account_id	AWS ID dell'account a cui appartiene l'ID dell'istanza
Nome dell'account	account_name	AWS nome dell'account
Stato dell'account	account_status	stato dell'account AMS
Conforme - Critico	comliant_critical	Numero di patch conformi con gravità «critica»
Conforme: elevato	comliant_high	Numero di patch conformi con severità «elevata»
Conforme: medio	comliant_medium	Numero di patch conformi con severità «media»
Conforme: basso	comliant_low	Numero di patch conformi con severità «bassa»
Conforme: informativo	comliant_informativo	Numero di patch conformi con severità «informativa»
Conforme: non specificato	comliant_non specificato	Numero di patch conformi con gravità «non specificata»
Conforme: totale	totale_conforme	Numero di patch conformi (tutte le severità)
Id dell'istanza	instance_id	ID dell' EC2 istanza
Nome dell'istanza	nome_istanza	Nome dell'istanza EC2
	account_sla	Livello di servizio dell'account AMS

Nome del campo	Nome del campo del set di dati	Definizione
Tipo di piattaforma di istanza	instance_platform_type	Tipo di sistema operativo (OS)
Nome della piattaforma dell'istanza	instance_platform_name	Nome del sistema operativo (OS)
Tipo di gruppo di patch di istanze	instance_patch_group_type	PREDEFINITO: gruppo di patch predefinito con finestra di manutenzione predefinita, determinato dal tag:TRUE sull'istanza AMSDefault PatchGroup CLIENTE: gruppo di patch creato dal cliente NOT_ASSIGNED: nessun gruppo di patch assegnato
Gruppo di patch di istanze	instance_patch_group	Nome del gruppo di patch utilizzato per raggruppare le istanze e applicare la stessa finestra di manutenzione
Stato dell'istanza	instance_state	Stato all'interno del ciclo di vita dell'istanza EC2
Tag di istanza	ec2_tags	I tag associati all'ID dell' EC2 istanza Amazon
Finestra di manutenzione dell'ultima esecuzione	last_execution_window	L'ultima volta in cui è stata eseguita la finestra di manutenzione
ID della finestra di manutenzione	window_id	ID finestra di manutenzione

Nome del campo	Nome del campo del set di dati	Definizione
Stato della finestra di manutenzione	window_state	stato della finestra di manutenzione
Tipo di finestra di manutenzione	tipo_finestra	Tipo di finestra di manutenzione
Finestra di manutenzione Data e ora di esecuzione successiva	window_next execution_time	La prossima volta è prevista l'esecuzione della finestra di manutenzione
Durata della finestra di manutenzione (ore)	finestra_duration	La durata della finestra di manutenzione in ore
Copertura della finestra di manutenzione	mw_covered_flag	Se un'istanza ha almeno una finestra di manutenzione abilitata con date di esecuzione future, viene considerata coperta, altrimenti non coperta
Non conforme: critico	noncomliant_critical	Numero di patch non conformi con gravità «critica»
Non conforme: elevato	noncomliant_high	Numero di patch non conformi con gravità «elevata»
Non conforme: medio	noncomliant_medium	Numero di patch non conformi con gravità «media»
Non conforme: basso	non conforme (basso)	Numero di patch non conformi con gravità «bassa»
Non conforme: informativo	non conforme _informativo	Numero di patch non conformi con severità «informativa»

Nome del campo	Nome del campo del set di dati	Definizione
Non conforme: non specificato	non conforme _non specificato	Numero di patch non conformi con gravità «non specificata»
Non conforme: totale	noncomliant_total	Numero di patch non conformi (tutte le severità)
ID di base della patch	patch_baseline_id	Linea di base della patch attualmente associata all'istanza
Stato della patch	patch_status	Stato generale di conformità delle patch. Se manca almeno una patch, l'istanza viene considerata non conforme, altrimenti conforme.
Account di produzione	prod_account	Identificatore degli account AMS prod e non prod, a seconda che il nome dell'account includa o meno il valore «PROD», «NONPROD».
Tipo di pila	instance_stack_type	Stack AMS (infrastruttura AMS all'interno dell'account del cliente) o Customer stack (infrastruttura gestita da AMS che supporta le applicazioni dei clienti)
	window_next_exec_yyyy	Un anno fa parte di window_next_execution_time
	finestra_next_exec_mm	Fa parte del mese di window_next_execution_time

Nome del campo	Nome del campo del set di dati	Definizione
	Window_next_exec_d	Fa parte del giorno di window_next_execution_time
	finestra_successiva _exec_HMI	Ora:parte in minuti di window_next_execution_time

Istanze in cui non sono state apportate le patch

Questo rapporto fornisce dettagli sulle istanze che non hanno ricevuto le patch durante l'ultima finestra di manutenzione.

Questo rapporto fornisce:

- Dati sulle patch mancanti a livello di ID della patch.
- Dati su tutte le istanze con almeno una patch mancante e attributi come la gravità della patch, i giorni senza patch, l'intervallo e la data di rilascio della patch.

Nome del campo	Nome del campo del set di dati	Definizione
Data/ora del rapporto	dataset_datetime	La data e l'ora di generazione del report
ID dell'account	aws_account_id	AWS ID dell'account a cui appartiene l'ID dell'istanza
Nome dell'account	account_name	AWS nome dell'account
Nome cliente Genitore	customer_name_parent	
Nome cliente	nome_cliente	
Account di produzione	prod_account	Identificatore degli account AMS prod o non prod, a

Nome del campo	Nome del campo del set di dati	Definizione
		seconda che il nome dell'acco unt includa il valore «PROD» o «NONPROD».
Stato dell'account	account_status	stato dell'account AMS
Tipo di account	tipo_conto	
	account_sla	Livello di servizio dell'account AMS
ID dell'istanza	instance_id	ID della tua EC2 istanza
Nome dell'istanza	nome_istanza	Nome della tua istanza EC2
Tipo di piattaforma dell'istanza	instance_platform_type	Tipo di sistema operativo (OS)
Stato dell'istanza	instance_state	Stato all'interno del ciclo di vita dell'istanza EC2
Tag di istanza	ec2_tags	I tag associati all'ID dell' EC2 istanza Amazon
ID della patch	patch_id	ID della patch rilasciata
Severità della patch	patch_sev	Severità della patch per editore
Classificazione delle patch	patch_class	Classificazione delle patch in base all'editore della patch
Data e ora di rilascio della patch (UTC)	release_dt_utc	Data di rilascio della patch per editore
Stato di installazione della patch	install_state	Installa lo stato della patch sull'istanza per SSM

Nome del campo	Nome del campo del set di dati	Definizione
Giorni senza patch	giorni senza patch	Numero di giorni in cui l'istanza è stata priva di patch dall'ultima scansione SSM
Intervallo di giorni senza patch	days_unpatched_bucket	Un sacco di giorni senza patch

Rapporto di Backup (giornaliero)

Il rapporto di backup copre le regioni primarie e secondarie (se applicabile). Copre lo stato dei backup (successo/fallimento) e i dati sulle istantanee scattate.

Questo rapporto fornisce:

- Stato del backup
- Numero di istantanee scattate
- Punto di ripristino
- Informazioni sul piano di backup e sul vault

Nome del campo	Nome del campo del set di dati	Definizione
Data/ora del rapporto	dataset_datetime	La data e l'ora di generazione del report.
ID dell'account	aws_account_id	ID account AWS a cui appartiene l'ID dell'istanza
ID dell'account amministratore	aws_admin_account_id	Account affidabile abilitato da te. AWS Organizations
Nome dell'account	account_name	Nome dell'account AWS
SLA dell'account	account_sla	Impegno al servizio dell'acco unt AMS

Nome del campo	Nome del campo del set di dati	Definizione
	malz_flag	Contrassegna l'account relativo a MALZ
	malz_role	ruolo MALZ
	restrizioni_accesso	Regioni a cui l'accesso è limitato
Data/ora di inizio pianificata dello snapshot di backup	start_by_dt_utc	Indicatore temporale in cui è pianificato l'inizio dell'ista ntanea
Data/ora di inizio effettiva dell'istantanea di backup	creation_dt_utc	Indicatore temporale in cui l'istantanea inizia effettiva mente
Data/ora di completamento dello snapshot di backup	completion_dt_utc	Timestamp al momento del completamento dell'istantanea
Data/ora di scadenza dello snapshot di backup	expiration_dt_utc	Indicatore temporale alla scadenza dell'istantanea
Stato del Backup Job	backup_job_status	Stato dell'istantanea
Tipo di backup	tipo_backup	Tipo di backup
ID Job di Backup	backup_job_id	L'identificatore univoco del job di backup
Dimensioni di backup in byte	backup_size_in_bytes	La dimensione del backup in byte
Piano di backup ARN	backup_plan_arn	Il piano di backup ARN
ID del piano di backup	backup_plan_id	Identificatore univoco del piano di backup

Nome del campo	Nome del campo del set di dati	Definizione
Nome del piano di backup	nome_piano di backup	Il nome del piano di Backup
Versione del piano di backup	versione del piano di backup	La versione del piano di backup
ID regola di backup	backup_rule_id	L'id della regola di backup
ARN di Backup Vault	backup_vault_arn	ARN del vault di backup
Nome del vault di backup	nome_vault_backup_	Il nome del backup vault
Ruolo IAM ARN	iam_role_arn	Il ruolo IAM (ARN)
Id dell'istanza	instance_id	ID univoco dell'istanza
Stato dell'istanza	instance_state	Stato istanza
Tag di istanza	ec2_tags	I tag associati all'ID dell'istanza EC2
ARN risorsa	resource_arn	Il nome della risorsa Amazon
ID della risorsa	resource_id	L'identificatore univoco della risorsa
Regione delle risorse	resource_region	Le aree primarie (e secondarie, se applicabile) della risorsa.
Tipo di risorsa	tipo_risorsa	Il tipo di risorsa
ARN del punto di ripristino	recovery_point_arn	L'ARN del punto di ripristino
ID del punto di ripristino	recovery_point_id	L'identificatore univoco del punto di ripristino
Stato del punto di ripristino	recovery_point_status	Stato del punto di ripristino

Nome del campo	Nome del campo del set di dati	Definizione
Eliminazione del punto di ripristino dopo giorni	recovery_point_delete_after_days	Eliminazione del punto di ripristino dopo giorni
Il punto di ripristino passa alla conservazione a freddo dopo giorni	recovery_point_move_to_cold_storage_after_days	Numero di giorni dopo la data di completamento in cui lo snapshot di backup viene spostato in cold storage
Stato della crittografia del punto di ripristino	recovery_point_is_encrypted	stato di crittografia del punto di ripristino
Chiave di crittografia del punto di ripristino (ARN)	recovery_point_encryption_key_arn	Chiave di crittografia del punto di ripristino ARN
ID dello stack	stack_id	Identificatore univoco dello stack di Cloudformation
Nome stack	stack_name	Nome stack
Tag: Gruppo di patch predefinito AMS	tag_ams_default_patch_group	Valore del tag: AMS Default Patch Group
Tag: App Id	tag_app_id	Valore del tag: ID app
Tag: nome dell'app	tag_app_name	Valore del tag: nome dell'app
Tag: Backup	tag_backup	Valore del tag: Backup
Tag: Compliance Framework	tag_compliance_framework	Valore del tag: Compliance Framework
Tag: Centro di costo	tag_cost_center	Valore del tag: Centro di costo
Tag: Cliente	tag_cliente	Valore del tag: cliente
Tag: Classificazione dei dati	tag_data_classification	Valore del tag: classificazione dei dati

Nome del campo	Nome del campo del set di dati	Definizione
Tag: Tipo di ambiente	tag_environment_type	Valore del tag: tipo di ambiente
Tag: Orario di apertura	tag_ore_di funzionamento	Valore del tag: ore di funzionamento
Tag: Owner Team	tag_owner_team	Valore del tag: Owner Team
Tag: Email del team del proprietario	tag_owner_team_email	Valore del tag: Owner Team Email
Tag: Patch Group	tag_patch_group	Valore del tag: Patch Group
Tag: Support Priority	tag_support_priority	Valore del tag: Support Priority
Stato del volume	volume_state	Stato del volume

Rapporto sull'incidente (settimanale)

Questo rapporto fornisce l'elenco aggregato degli incidenti insieme alla priorità, alla gravità e allo stato più recente, tra cui:

- Dati sui casi di assistenza classificati come incidenti sull'account gestito
- Informazioni sugli incidenti necessarie per visualizzare le metriche degli incidenti per l'account gestito
- Dati sulle categorie di incidenti e sullo stato di riparazione di ogni incidente

Sia la visualizzazione che i dati sono disponibili per il rapporto settimanale sugli incidenti.

- È possibile accedere alla visualizzazione tramite la console AMS dell'account tramite la pagina Report.
- È possibile accedere al set di dati con lo schema seguente tramite il bucket S3 nell'account gestito.
- Utilizza i campi di data forniti per filtrare gli incidenti in base al mese, trimestre, settimana, and/or giorno in cui l'incidente è stato creato o risolto.

Nome del campo	Nome del campo del set di dati	Definizione
Data/ora del rapporto	dataset_datetime	La data e l'ora di generazione del report.
ID dell'account	aws_account_id	AWS ID dell'account a cui appartiene l'incidente.
ID dell'account amministratore	aws_admin_account_id	Account affidabile abilitato da te. AWS Organizations
Nome dell'account	account_name	AWS nome dell'account.
ID del caso	case_id	L'ID dell'incidente.
Mese di creazione	created_month	Il mese in cui è stato creato l'incidente.
Priorità	priority	La priorità dell'incidente.
Gravità	severity	La gravità dell'incidente.
Stato	stato	Lo stato dell'incidente.
Categoria	yuma_category	La categoria dell'incidente.
Giorno di creazione	giorno_creato	Il giorno in cui l'incidente è stato creato nel formato. YYYY-MM-DD
Settimana creata	created_wk	La settimana in cui l'inciden te è stato creato nel formato YYYYY-WW. Da domenica a sabato vengono contati come inizio e fine settimana. La settimana va dalla 01 alla 52. La settimana 01 è sempre la settimana che contiene il primo giorno dell'anno

Nome del campo	Nome del campo del set di dati	Definizione
		. Ad esempio, 2023-12-3 1 e 2024-01-01 sono nella settimana 2024-01.
Trimestre creato	created_qtr	Il trimestre in cui l'incidente è stato creato nel formato YYYYY-Q. Dal 01/01 al 31/03 è definito come Q1 e così via.
Giorno risolto	giorno_risolto	Il giorno in cui l'incidente è stato risolto in formato. YYYY-MM-DD
Settimana risolta	resolved_wk	La settimana in cui l'inciden te è stato risolto nel formato YYYYY-WW. Da domenica a sabato vengono contati come inizio e fine settimana. La settimana va dalla 01 alla 52. La settimana 01 è sempre la settimana che contiene il primo giorno dell'anno. Ad esempio, il 2023-12-31 e il 2024-01-01 sono nella settimana 2024-01.
Mese risolto	resolved_month	Il mese in cui l'incidente è stato risolto nel formato YYYY-MM.
Trimestre risolto	resolved_qtr	Il trimestre in cui l'incidente è stato risolto nel formato YYYYY-Q. Dal 01/01 al 31/03 è definito come Q1 e così via.

Nome del campo	Nome del campo del set di dati	Definizione
Regola di raggruppamento creata	grouping_rule	La regola di raggruppamento che si applica all'incidente. O «no_grouping» o «instance _grouping».
Istanza IDs	instance_ids	L'istanza associata all'incid ente.
Numero di avvisi	numero_di_avvisi	Il numero di avvisi associati a quell'incidente. Se hai abilitato il raggruppamento, questo numero può essere maggiore di 1. Se il raggruppamento non è abilitato, sarà sempre 1.
Creato alle	created_at	Il timestamp in cui è stato creato l'incidente.
Allarme ARNs	alarm_arns	L'Amazon Resource Name («arn») degli allarmi associati al tuo incidente.
Allarmi correlati	related_alarms	I nomi leggibili dall'uomo di tutti gli allarmi associati all'incidente.

Rapporto di fatturazione (mensile)

Dettagli sugli addebiti di fatturazione

Questo report fornisce dettagli sugli addebiti di fatturazione di AMS con account collegati e rispettivi servizi AWS.

Questo rapporto fornisce:

- Dati sui costi a livello di servizio AMS, sulle percentuali di upgrade, sui livelli di servizio AMS a livello di account e sulle tariffe AMS.
- Dati sugli account collegati e sui costi di utilizzo di AWS.

> **Important**
>
> Il rapporto di fatturazione mensile è disponibile solo nel tuo account di gestione dei pagamenti (MPA) o nel tuo account di addebito definito. Questi sono gli account a cui viene inviata la fattura mensile AMS. Se non riesci a individuare questi account, contatta il tuo Cloud Service Delivery Manager (CSDM) per ricevere assistenza.

Nome del campo	Nome del campo del set di dati	Definizione
Data di fatturazione	data	Il mese e l'anno del servizio fatturato
ID del conto di pagamento	payer_account_id	L'ID a 12 cifre che identific a l'account responsabile del pagamento degli addebiti AMS
ID dell'account collegato	linked_account_id	L'ID a 12 cifre che identifica l'account AMS che utilizza i servizi che genera espansioni
AWS Nome del servizio	product_name	Il AWS servizio che è stato utilizzato
AWS Addebiti	aws_charges	I AWS costi per il nome del AWS servizio in Service Name AWS
Piano tariffario	piano_tariffario	Il piano tariffario associato all'account collegato

Nome del campo	Nome del campo del set di dati	Definizione
Gruppo di assistenza AMS	tier_uplifting_groups	Codice del gruppo di servizi AMS che determina la percentuale di uplift
Proporzione di sollevamento	uplift_percent	La percentuale di aggiornamento (in formato decimale V.WXYZ) basata su pricing_plan, SLA e service AWS
AWS Addebiti adeguati	adjusted_aws_usage	AWS utilizzo adattato per AMS
Costi aumentati AWS	uplifted_aws_charges	La percentuale degli AWS addebiti da addebitare per AMS; adjusted_aws_charges * uplift_percent
Istanze RDS Spend EC2	instances_ec2_rds_spend	Istanze Spend on e RDS EC2
Costi per istanze riservate	ris_charges	Costi per istanze riservate
Costi aumentati per le istanze riservate	uplifted_ris	La percentuale dei costi delle istanze riservate da addebitare per AMS; ris_charges * uplift_percent
Costi del Savings Plan	sp_charges	SavingsPlan costi di utilizzo
Costi del piano Uplifted Savings Plan	uplifted_sp	La percentuale degli addebiti dei piani di risparmio da addebitare per AMS; sp_charges * uplift_percent
Tariffe AMS	ams_charges	Costi totali ams per il prodotto; uplifted_aws_charges + instance_ec2_rds_spend + uplifted_ris + uplifted_sp

Nome del campo	Nome del campo del set di dati	Definizione
Tariffa minima ripartita proporzionalmente	ripartito_minimo	L'importo che addebitiamo per soddisfare il minimo contrattuale
Costi totali AMS dell'account collegato	linked_account_total ams_charges	Somma di tutti gli addebiti per il linked_account
Costi totali AMS del conto di pagamento	payer_account_total ams_charges	Somma di tutti gli addebiti relativi al conto di pagamento
Tariffa minima	tariffe_minime	Commissioni minime AMS (se applicabile)
Sconto Reserved Instance e Savings Plan	adj_ri_sp_charges	RI/SP discount to be applied against RI/SPaddebiti (applicabili in determinate circostanze)

Rapporti aggregati

I report self-service aggregati (SSR) offrono una visualizzazione dei report self-service esistenti aggregati a livello di organizzazione, su più account. Questo vi offre visibilità sulle principali metriche operative, come la conformità delle patch, la copertura dei backup e gli incidenti, su tutti gli account gestiti da AMS all'interno della vostra azienda. AWS Organizations

L'SSR aggregato è disponibile in tutte le attività commerciali in Regioni AWS cui è disponibile AWS Managed Services. Per un elenco completo delle regioni disponibili, consulta la tabella delle regioni.

Abilita i report aggregati

È necessario gestire l'SSR aggregato da un account di gestione. AWS Organizations L'account di gestione è l' AWS account che hai usato per creare la tua organizzazione.

Per abilitare l'SSR aggregato per un account di AWS Organizations gestione integrato in AMS, accedi alla console AMS e vai a Reports. Seleziona Organization Access nell' top-right-handangolo per aprire il riquadro AWS Managed Services Console: Organization View. Da questo riquadro, puoi gestire la funzionalità Aggregated SSR.

AWS Organizations gli account di gestione che non sono integrati in AMS non hanno accesso alla console AMS. Per abilitare Aggregated SSR per un account di AWS Organizations gestione non registrato su AMS, esegui prima l'autenticazione sul tuo Account AWS, quindi accedi alla AWS console e cerca Managed Services. Si apre la pagina AMS Marketing. In questa pagina, seleziona il link Organization Access nella barra di navigazione per aprire la console AWS Managed Services: Organization View, dove puoi gestire la funzionalità Aggregated SSR.

La prima volta che accedi alla console AWS Managed Services: Organization View, completa i seguenti passaggi:

1. Se non l'hai già configurata AWS Organizations, scegli Abilita AWS Organizations dalla tua console. Per ulteriori informazioni sulla configurazione AWS Organizations, consulta la Guida AWS Organizations per l'utente. Puoi saltare questo passaggio se lo usi AWS Organizations già.
2. Per abilitare il servizio Aggregated Self-Service Reporting, seleziona Abilita accesso affidabile sulla console.
3. (Facoltativo) Registra un amministratore delegato per avere accesso in lettura alla visualizzazione organizzativa.

Visualizza i report aggregati come amministratore delegato

Un amministratore delegato è l'account scelto per l'accesso in lettura ai report aggregati. L'amministratore delegato deve essere un account registrato su AMS ed essere l'unico account con accesso in lettura ai report aggregati.

Per scegliere un amministratore delegato, inserisci l'ID dell'account nel passaggio 3 nella Console AWS Managed Services: Organization View. Puoi avere un solo account amministratore delegato registrato alla volta. Tieni presente che l'account amministratore delegato deve essere un account gestito da AMS.

Per aggiornare un account amministratore delegato, accedi alla Console AWS Managed Services: Organization View e seleziona Rimuovi l'amministratore delegato. La console richiede di inserire un nuovo ID account per registrarti come amministratore delegato.

Leggi i report aggregati

Se non registri un amministratore delegato e il tuo account di AWS Organizations gestione viene inserito in AMS, per impostazione predefinita l'account di AWS Organizations gestione ottiene l'accesso in lettura ai report aggregati. Se l'account di AWS Organizations gestione non è gestito da AMS, devi scegliere un account amministratore delegato per avere accesso in lettura ai report aggregati.

In qualsiasi momento, solo un singolo account inserito in AMS ha accesso in lettura ai report aggregati, sia l'account di AWS Organizations gestione che l'amministratore delegato registrato. Tutti gli altri account membri all'interno dell'organizzazione (e inseriti in AMS) hanno ancora accesso solo ai report relativi a un singolo account per ogni singolo account.

Dopo aver abilitato l'SSR aggregato, accedi ai tuoi Rapporti. Tutti i report self-service esistenti sono elencati in questa sezione e un tag blu indica che sono stati aggregati. Tieni presente che devi accedere alla console AMS dall'account che hai scelto per avere accesso in lettura ai report aggregati. Si tratta dell'account di AWS Organizations gestione o dell'account amministratore delegato.

Dopo aver abilitato l'SSR aggregato, i report aggregati sono disponibili a partire dal ciclo di rendicontazione successivo.

Disattiva i report aggregati

Per disabilitare Aggregated SSR, apri la Console AWS Managed Services: Organization View. Seleziona Disabilita l'accesso affidabile. Dopo aver disabilitato l'accesso affidabile per Aggregated SSR, i report self-service AMS smettono di essere aggregati a livello di organizzazione, tra gli account. Tieni inoltre presente che la disattivazione ha effetto a partire dal successivo ciclo di segnalazione.

Dopo aver disabilitato l'SSR aggregato, è necessario attendere che i report nella console AMS vengano visualizzati come report per account singolo. Questo ritardo si verifica perché la disattivazione della funzionalità ha effetto a partire dal ciclo di segnalazione successivo.

Dashboard di report self-service AMS

I report self-service AMS offrono due dashboard: e. Dashboard Resource Tagger Dashboard Security Config Rules

Dashboard Resource Tagger

La dashboard di AMS Resource Tagger fornisce informazioni dettagliate sulle risorse supportate da Resource Tagger, nonché sullo stato attuale dei tag che Resource Tagger è configurato per applicare a tali risorse.

Copertura di Resource Tagger per tipo di risorsa

Questo set di dati è costituito da un elenco di risorse con tag gestiti da Resource Tagger.

La copertura delle risorse per tipo di risorsa viene visualizzata come quattro grafici a linee che descrivono le seguenti metriche:

- Numero di risorse: il numero totale di risorse nella regione, per tipo di risorsa.
- Risorse con tag gestiti mancanti: il numero totale di risorse nella regione, per tipo di risorsa, che richiedono tag gestiti ma non sono etichettate da Resource Tagger.
- Risorse non gestite: il numero totale di risorse nella regione, per tipo di risorsa, a cui non sono stati applicati tag gestiti da Resource Tagger. Ciò significa in genere che queste risorse non corrispondono a nessuna configurazione di Resource Tagger o sono esplicitamente escluse dalle configurazioni.
- Risorse gestite: analoga alla metrica delle risorse non gestite (Resource Count - Unmanaged Resources).

La tabella seguente elenca i dati forniti da questo rapporto.

Nome del campo	Nome del campo del set di dati	Definizione
Data/ora del rapporto	dataset_datetime	Data e ora di generazione del report (ora UTC)
Account AWS ID	aws_account_id	Account AWS ID
ID account amministratore	aws_admin_account_id	Account affidabile abilitato da te. AWS Organizations
Region	region	Regione AWS

Nome del campo	Nome del campo del set di dati	Definizione
Tipo di risorsa	resource_type	Questo campo identifica il tipo di risorsa. Sono inclusi solo i tipi di risorse supportati da Resource Tagger.
Numero di risorse	resource_count	Numero di risorse (del tipo di risorsa specificato) distribuite in questa regione.
ResourcesMissingManagedTags	resource_missing_managed_tags_count	Numero di risorse (del tipo di risorsa specificato) che richiedono tag gestiti, in base ai profili di configurazione, ma non sono ancora state taggate da Resource Tagger.
UnmanagedResources	unmanaged_resource_count	Numero di risorse (del tipo di risorsa specificato) senza tag gestiti applicati da Resource Tagger. In genere, queste risorse non corrispondono a nessun blocco di configurazione di Resource Tagger o sono esplicitamente escluse dai blocchi di configurazione.

Conformità alle regole di configurazione Resource Tagger

Questo set di dati è costituito da un elenco di risorse in un Regione AWS determinato tipo di risorsa a cui è applicato un determinato profilo di configurazione. Viene visualizzato come un grafico a linee.

La tabella seguente elenca i dati forniti da questo rapporto.

Nome del campo	Nome del campo del set di dati	Definizione
Data/ora del rapporto	dataset_datetime	Data e ora di generazione del report (ora UTC)
Account AWS ID	aws_account_id	Account AWS ID
ID account amministratore	aws_admin_account_id	Account affidabile abilitato da te. AWS Organizations
Region	region	Regione AWS
Tipo di risorsa	resource_type	Questo campo identifica il tipo di risorsa. Sono inclusi solo i tipi di risorse supportati da Resource Tagger.
ID del profilo di configurazione	configuration_profile_id	L'ID del profilo di configurazione Resource Tagger. Un profilo di configurazione viene utilizzato per definire le politiche e le regole utilizzate per etichettare le risorse.
MatchingResourceCount	resource_count	Numero di risorse (del tipo di risorsa specificato) che corrispondono all'ID del profilo di configurazione Resource Tagger. Affinché una risorsa corrisponda al profilo di configurazione, il profilo deve essere abilitato e la risorsa deve corrispondere alla regola del profilo.

Risorse non conformi a Resource Tagger

Questo set di dati è costituito da un elenco di risorse non conformi per una singola configurazione di Resource Tagger. Questi dati sono un'istantanea quotidiana della conformità delle risorse e mostrano lo stato delle risorse dei clienti nel momento in cui questi report vengono consegnati agli account dei clienti (non è disponibile una visualizzazione storica). Viene visualizzato come una tabella pivot composta da risorse non conformi a una determinata configurazione.

La tabella seguente elenca i dati forniti da questo rapporto.

Nome del campo	Nome del campo del set di dati	Definizione
Data/ora del rapporto	dataset_datetime	Data e ora di generazione del report (ora UTC)
Account AWS ID	aws_account_id	Account AWS ID
ID account amministratore	aws_admin_account_id	Account affidabile abilitato da te. AWS Organizations
Region	region	Regione AWS
Tipo di risorsa	resource_type	Questo campo identifica il tipo di risorsa. Sono inclusi solo i tipi di risorse supportati da Resource Tagger.
Resource ID (ID risorsa)	resource_id	L'identificatore univoco per le risorse supportate da Resource Tagger.
Stato di copertura	coverage_state	Questo campo indica se la risorsa è etichettata come configurato dall'ID di configura zione Resource Tagger.
ID del profilo di configurazione	configuration_profile_id	L'ID del profilo di configura zione Resource Tagger. Un profilo di configurazione

Nome del campo	Nome del campo del set di dati	Definizione
		viene utilizzato per definire le politiche e le regole utilizzate per etichettare le risorse.

Dashboard Security Config Rules

Il Security Config Rules Dashboard fornisce una panoramica approfondita sulla conformità delle risorse e delle regole degli AWS Config account AMS. Puoi filtrare il rapporto in base alla gravità della regola per dare priorità ai risultati più critici. La tabella seguente elenca i dati forniti da questo rapporto.

Nome del campo	Nome del campo del set di dati	Definizione
Account AWS ID	Account AWS ID	L'ID dell'account legato alle risorse correlate.
ID dell'account amministratore	aws_admin_account_id	Account affidabile abilitato da te. AWS Organizations
rapporto data/ora	Data del rapporto	Data e ora di generazione del rapporto.
customer_name	Nome del cliente	Il nome del cliente.
account_name	Nome dell'account	Il nome associato all'ID dell'account
resource_id	Resource ID (ID risorsa)	Un identificatore per una risorsa.
resource_region	Regione delle risorse	La posizione Regione AWS in cui si trova la risorsa.

Nome del campo	Nome del campo del set di dati	Definizione
resource_type	Tipo di risorsa	Il tipo di risorsa Servizio AWS o.
nome_risorsa	Nome risorsa	Il nome della risorsa.
resource_ams_flag	Bandiera AMS di risorsa	Se la risorsa è di proprietà di AMS, questo flag è impostato su TRUE. Se la risorsa è di proprietà del cliente, questo flag è impostato su FALSE. Se la proprietà non è nota, questo flag è impostato su UNKNOWN.
config_rule	Regola di configurazione	Il nome non personalizzabile per la regola di configurazione.
config_rule_description	Descrizione della regola di configurazione	Una descrizione della regola di configurazione.
source_identifier	Identificatore di origine	Un identificatore univoco per la regola di configurazione gestita e nessun identificatore per una regola di configura zione personalizzata.
compliance_flag	Bandiera di conformità	Mostra se le risorse sono conformi o non conformi alle regole di configurazione.
tipo_regola	Tipo di regola	Indica se la regola è predefini ta o personalizzata.

Nome del campo	Nome del campo del set di dati	Definizione
eccezione_flag	Bandiera di eccezione	Il flag di eccezione della risorsa mostra l'accettazione del rischio nei confronti di una risorsa non conforme. Se il flag di eccezione della risorsa è TRUE per una risorsa, la risorsa viene esentata. Se il flag di eccezione è NULL, la risorsa non è esentata.
cal_dt	Data	La data di valutazione della regola.
descrizione_riparazione	Descrizione della riparazione	Una descrizione di come porre rimedio alla conformità alle regole.
severity	Gravità	La severità delle regole di configurazione indica l'impatto della non conformità.
azione_cliente	Azione del cliente	Azioni necessarie per porre rimedio a questa regola.
raccomandazione	Raccomandazione	Una descrizione di ciò che verifica la regola di configura zione.
categoria_di riparazione	Categoria di riparazione	Le azioni predefinite che AMS intraprende quando questa regola diventa non conforme.

Policy di conservazione dei dati

AMS SSR applica una politica di conservazione dei dati per rapporto. Dopo il periodo di riferimento, i dati vengono cancellati e non sono più disponibili.

Nome del rapporto	Console SSR per la conservazione dei dati	Bucket SSR S3 per la conservazione dei dati
Riepilogo dei dettagli dell'istanza per AMS Patching	2 mesi	2 anni
Dettagli della patch	2 mesi	2 anni
Istanze in cui non sono state apportate le patch durante l'esecuzione della finestra di manutenzione	2 mesi	2 anni
Dettagli sulle spese di fatturazione AMS	2 anni	2 anni
Report di Backup giornaliero	1 mese	2 anni
Rapporto settimanale sugli incidenti	2 mesi	2 anni
Dashboard delle regole di configurazione di sicurezza	3 mesi	2 anni
Dashboard Resource Tagger	1 anno	2 anni

Fuori bordo da SSR

Per abbandonare il servizio SSR, crea una richiesta di servizio (SR) tramite la console AMS. Dopo aver inviato il SR, un tecnico operativo AMS ti aiuterà a uscire dall'SSR. Nella SR, indica il motivo per cui desideri abbandonare l'imbarco.

Per trasferire un account ed eseguire una pulizia delle risorse, crea un SR tramite la console AMS. Dopo aver inviato il SR, un tecnico operativo AMS ti aiuterà a eliminare il bucket SSR Amazon S3.

Se esci da AMS, vieni automaticamente espulso dalla console AMS SSR. AMS interrompe automaticamente l'invio di dati al tuo account. AMS elimina il bucket SSR S3 come parte del processo di offboarding.

Gestione degli accessi in AMS Accelerate

La gestione degli accessi è il modo in cui le risorse vengono protette, permettendo solo l'accesso autorizzato e autenticato. Con AMS Accelerate, sei responsabile della gestione dell'accesso alle tue Account AWS e alle relative risorse sottostanti, come le soluzioni di gestione degli accessi, le politiche di accesso e i processi correlati. Per aiutarti a gestire la tua soluzione di accesso, AMS Accelerate implementa AWS Config regole che rilevano le configurazioni errate più comuni di IAM e quindi fornisce notifiche di correzione. Un errore di configurazione comune di IAM è rappresentato dal fatto che l'utente root dispone delle chiavi di accesso. La regola di `iam-root-access-key-check` configurazione verifica se la chiave di accesso dell'utente root è disponibile ed è conforme o se la chiave di accesso non esiste. Per un elenco delle regole di configurazione distribuite da AMS, consulta la libreria delle regole AMS. AWS Config

Argomenti

- Accedi alla console Accelerate
- Autorizzazioni per l'utilizzo delle funzionalità AMS
- Perché e quando AMS accede al tuo account
- In che modo AMS accede al tuo account
- Come e quando usare l'account utente root in AMS

Accedi alla console Accelerate

Quando entri a bordo con Accelerate, hai automaticamente accesso alla console Accelerate. Puoi accedere alla console cercando Managed Services nella tua console di gestione AWS. La console Accelerate offre una panoramica riassuntiva delle funzionalità disponibili con Accelerate. Questa visualizzazione include i singoli componenti presentati nella dashboard e nelle pagine di configurazione.

Autorizzazioni per l'utilizzo delle funzionalità AMS

Per consentire agli utenti di leggere e configurare le funzionalità di AMS Accelerate, come l'accesso alla console AMS o la configurazione dei backup, è necessario concedere autorizzazioni esplicite ai rispettivi ruoli IAM per eseguire tali azioni. Il seguente CloudFormation modello contiene le politiche necessarie per leggere e configurare i servizi associati ad AMS in modo da poterli assegnare ai ruoli IAM. Sono progettati per allinearsi strettamente alle responsabilità lavorative comuni nel

settore IT, in cui sono richieste le autorizzazioni di amministratore o di sola lettura; tuttavia, se è necessario concedere autorizzazioni diverse agli utenti, è possibile modificare la politica per includere o escludere autorizzazioni specifiche. Puoi anche creare policy personalizzate.

Il modello fornisce due politiche. La `AMSAccelerateAdminAccess` policy è pensata per essere utilizzata per configurare e utilizzare i componenti AMS Accelerate. Questa politica viene in genere adottata da un amministratore IT e concede le autorizzazioni per configurare le funzionalità AMS come l'applicazione di patch e i backup. `AMSAccelerateReadOnly`Concede le autorizzazioni minime richieste per la visualizzazione delle risorse relative ad AMS Accelerate.

```
AWSTemplateFormatVersion: 2010-09-09
Description: AMSAccelerateCustomerAccessPolicies

Resources:
  AMSAccelerateAdminAccess:
    Type: 'AWS::IAM::ManagedPolicy'
    Properties:
      ManagedPolicyName: AMSAccelerateAdminAccess
      Path: /
      PolicyDocument:
        Fn::Sub:
        - |
          {
            "Version": "2012-10-17",
            "Statement": [
              {
                 "Sid": "AmsSelfServiceReport",
                 "Effect": "Allow",
                 "Action": "amsssrv:*",
                 "Resource": "*"
              },
              {
                "Sid": "AmsBackupPolicy",
                "Effect": "Allow",
                "Action": "iam:PassRole",
                "Resource": "arn:aws:iam::${AWS::AccountId}:role/ams-backup-iam-role"
              },
              {
                "Sid": "AmsChangeRecordKMSPolicy",
                "Effect": "Allow",
                "Action": [
                  "kms:Encrypt",
                  "kms:Decrypt",
```

```
                "kms:GenerateDataKey"
              ],
              "Resource": [
                "arn:aws:kms:${AWS::Region}:${AWS::AccountId}:key/*"
              ],
              "Condition": {
                "ForAnyValue:StringLike": {
                  "kms:ResourceAliases": "alias/AMSCloudTrailLogManagement"
                }
              }
            },
            {
              "Sid": "AmsChangeRecordAthenaReadPolicy",
              "Effect": "Allow",
              "Action": [
                "athena:BatchGetNamedQuery",
                "athena:Get*",
                "athena:List*",
                "athena:StartQueryExecution",
                "athena:UpdateWorkGroup",
                "glue:GetDatabase*",
                "glue:GetTable*",
                "s3:GetAccountPublicAccessBlock",
                "s3:ListAccessPoints",
                "s3:ListAllMyBuckets"
              ],
              "Resource": "*"
            },
            {
              "Sid": "AmsChangeRecordS3ReadPolicy",
              "Effect": "Allow",
              "Action": [
                "s3:Get*",
                "s3:List*"
              ],
              "Resource": [
                "arn:aws:s3:::ams-a${AWS::AccountId}-athena-results-${AWS::Region}",
                "arn:aws:s3:::ams-a${AWS::AccountId}-athena-results-${AWS::Region}/
*",
                "arn:aws:s3:::ams-a${AWS::AccountId}-cloudtrail-${AWS::Region}",
                "arn:aws:s3:::ams-a${AWS::AccountId}-cloudtrail-${AWS::Region}/*"
              ]
            },
            {
```

```
      "Sid": "AmsChangeRecordS3WritePolicy",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:PutObjectLegalHold",
        "s3:PutObjectRetention"

      ],
      "Resource": [
        "arn:aws:s3:::ams-a${AWS::AccountId}-athena-results-${AWS::Region}/*"
      ]
    },
    {
      "Sid": "MaciePolicy",
      "Effect": "Allow",
      "Action": [
        "macie2:GetFindingStatistics"
      ],
      "Resource": "*"
    },
    {
      "Sid": "GuardDutyPolicy",
      "Effect": "Allow",
      "Action": [
        "guardduty:GetFindingsStatistics",
        "guardduty:ListDetectors"
      ],
      "Resource": "*"
    },
    {
      "Sid": "SupportPolicy",
      "Effect": "Allow",
      "Action": "support:*",
      "Resource": "*"
    },
    {
      "Sid": "ConfigPolicy",
      "Effect": "Allow",
      "Action": [
        "config:Get*",
        "config:Describe*",
        "config:Deliver*",
        "config:List*",
        "config:StartConfigRulesEvaluation"
```

```
                ],
                "Resource": "*"
              },
              {
                "Sid": "AppConfigReadPolicy",
                "Effect": "Allow",
                "Action": [
                  "appconfig:List*",
                  "appconfig:Get*"
                ],
                "Resource": "*"
              },
              {
                "Sid": "AppConfigPolicy",
                "Effect": "Allow",
                "Action": [
                  "appconfig:StartDeployment",
                  "appconfig:StopDeployment",
                  "appconfig:CreateHostedConfigurationVersion",
                  "appconfig:ValidateConfiguration"
                ],
                "Resource": [
                  "arn:aws:appconfig:*:${AWS::AccountId}:application/
${AMSAlarmManagerConfigurationApplicationId}",
                  "arn:aws:appconfig:*:${AWS::AccountId}:application/
${AMSAlarmManagerConfigurationApplicationId}/configurationprofile/
${AMSAlarmManagerConfigurationCustomerManagedAlarmsProfileID}",
                  "arn:aws:appconfig:*:${AWS::AccountId}:application/
${AMSAlarmManagerConfigurationApplicationId}/environment/*",
                  "arn:aws:appconfig:*:${AWS::AccountId}:application/
${AMSResourceTaggerConfigurationApplicationId}",
                  "arn:aws:appconfig:*:${AWS::AccountId}:application/
${AMSResourceTaggerConfigurationApplicationId}/configurationprofile/
${AMSResourceTaggerConfigurationCustomerManagedTagsProfileID}",
                  "arn:aws:appconfig:*:${AWS::AccountId}:application/
${AMSResourceTaggerConfigurationApplicationId}/environment/*",
                  "arn:aws:appconfig:*:${AWS::AccountId}:deploymentstrategy/*"
                ]
              },
              {
                "Sid": "CloudFormationStacksPolicy",
                "Effect": "Allow",
                "Action": [
                  "cloudformation:DescribeStacks"
```

```
            ],
            "Resource": "*"
          },
          {
            "Sid": "EC2Policy",
            "Action": [
              "ec2:DescribeInstances"
            ],
            "Effect": "Allow",
            "Resource": "*"
          },
          {
            "Sid": "SSMPolicy",
            "Effect": "Allow",
            "Action": [
              "ssm:AddTagsToResource",
              "ssm:CancelCommand",
              "ssm:CancelMaintenanceWindowExecution",
              "ssm:CreateAssociation",
              "ssm:CreateAssociationBatch",
              "ssm:CreateMaintenanceWindow",
              "ssm:CreateOpsItem",
              "ssm:CreatePatchBaseline",
              "ssm:DeleteAssociation",
              "ssm:DeleteMaintenanceWindow",
              "ssm:DeletePatchBaseline",
              "ssm:DeregisterPatchBaselineForPatchGroup",
              "ssm:DeregisterTargetFromMaintenanceWindow",
              "ssm:DeregisterTaskFromMaintenanceWindow",
              "ssm:Describe*",
              "ssm:Get*",
              "ssm:List*",
              "ssm:PutConfigurePackageResult",
              "ssm:RegisterDefaultPatchBaseline",
              "ssm:RegisterPatchBaselineForPatchGroup",
              "ssm:RegisterTargetWithMaintenanceWindow",
              "ssm:RegisterTaskWithMaintenanceWindow",
              "ssm:RemoveTagsFromResource",
              "ssm:SendCommand",
              "ssm:StartAssociationsOnce",
              "ssm:StartAutomationExecution",
              "ssm:StartSession",
              "ssm:StopAutomationExecution",
              "ssm:TerminateSession",
```

```
            "ssm:UpdateAssociation",
            "ssm:UpdateAssociationStatus",
            "ssm:UpdateMaintenanceWindow",
            "ssm:UpdateMaintenanceWindowTarget",
            "ssm:UpdateMaintenanceWindowTask",
            "ssm:UpdateOpsItem",
            "ssm:UpdatePatchBaseline"
          ],
          "Resource": "*"
        },
        {
          "Sid": "AmsPatchRestrictAMSResources",
          "Effect": "Deny",
          "Action": [
            "ssm:DeletePatchBaseline",
            "ssm:UpdatePatchBaseline"
          ],
          "Resource": [
            "arn:aws:ssm:${AWS::Region}:${AWS::AccountId}:patchbaseline/*"
          ],
          "Condition": {
            "StringLike": {
              "aws:ResourceTag/ams:resourceOwner": "*"
            }
          }
        },
        {
          "Sid": "AmsPatchRestrictAmsTags",
          "Effect": "Deny",
          "Action": [
            "ssm:AddTagsToResource",
            "ssm:RemoveTagsFromResource"
          ],
          "Resource": "*",
          "Condition": {
            "ForAnyValue:StringLike": {
              "aws:TagKeys": [
                "AMS*",
                "Ams*",
                "ams*"
              ]
            }
          }
        },
```

```
            {
              "Sid": "TagReadPolicy",
              "Effect": "Allow",
              "Action": [
                "tag:GetResources",
                "tag:GetTagKeys"
              ],
              "Resource": "*"
            },
            {
              "Sid": "CloudtrailReadPolicy",
              "Effect": "Allow",
              "Action": [
                "cloudtrail:DescribeTrails",
                "cloudtrail:GetTrailStatus",
                "cloudtrail:LookupEvents"
              ],
              "Resource": "*"
            },
            {
              "Sid": "EventBridgePolicy",
              "Effect": "Allow",
              "Action": [
                "events:Describe*",
                "events:List*",
                "events:TestEventPattern"
              ],
              "Resource": "*"
            },
            {
              "Sid": "IAMReadOnlyPolicy",
              "Action": [
                  "iam:ListRoles",
                  "iam:GetRole"
              ],
              "Effect": "Allow",
              "Resource": "*"
            },
            {
              "Sid": "AmsResourceSchedulerPassRolePolicy",
              "Effect": "Allow",
              "Action": "iam:PassRole",
              "Resource": "arn:aws:iam::${AWS::AccountId}:role/
ams_resource_scheduler_ssm_automation_role",
```

```
                "Condition": {
                    "StringEquals": {
                        "iam:PassedToService": "ssm.amazonaws.com"
                    }
                }
              }
            ]
          }
        - AMSAlarmManagerConfigurationApplicationId: !ImportValue "AMS-Alarm-Manager-
Configuration-ApplicationId"
          AMSAlarmManagerConfigurationCustomerManagedAlarmsProfileID: !ImportValue
 "AMS-Alarm-Manager-Configuration-CustomerManagedAlarms-ProfileID"
          AMSResourceTaggerConfigurationApplicationId: !ImportValue "AMS-
ResourceTagger-Configuration-ApplicationId"
          AMSResourceTaggerConfigurationCustomerManagedTagsProfileID: !ImportValue
 "AMS-ResourceTagger-Configuration-CustomerManagedTags-ProfileID"

  AMSAccelerateReadOnly:
    Type: 'AWS::IAM::ManagedPolicy'
    Properties:
      ManagedPolicyName: AMSAccelerateReadOnly
      Path: /
      PolicyDocument: !Sub |
        {
          "Version": "2012-10-17",
          "Statement": [
          {
                "Sid": "AmsSelfServiceReport",
                "Effect": "Allow",
                "Action": "amsssrv:*",
                "Resource": "*"
              },
            {
               "Sid": "AmsBackupPolicy",
               "Effect": "Allow",
               "Action": [
                 "backup:Describe*",
                 "backup:Get*",
                 "backup:List*"
               ],
               "Resource": "*"
            },
            {
                "Action": [
```

```
                "rds:DescribeDBSnapshots",
                "rds:ListTagsForResource",
                "rds:DescribeDBInstances",
                "rds:describeDBSnapshots",
                "rds:describeDBEngineVersions",
                "rds:describeOptionGroups",
                "rds:describeOrderableDBInstanceOptions",
                "rds:describeDBSubnetGroups",
                "rds:DescribeDBClusterSnapshots",
                "rds:DescribeDBClusters",
                "rds:DescribeDBParameterGroups",
                "rds:DescribeDBClusterParameterGroups",
                "rds:DescribeDBInstanceAutomatedBackups"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "dynamodb:ListBackups",
                "dynamodb:ListTables"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "elasticfilesystem:DescribeFilesystems"
            ],
            "Resource": "arn:aws:elasticfilesystem:*:*:file-system/*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "ec2:DescribeSnapshots",
                "ec2:DescribeVolumes",
                "ec2:describeAvailabilityZones",
                "ec2:DescribeVpcs",
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeImages",
                "ec2:DescribeSubnets",
                "ec2:DescribePlacementGroups",
                "ec2:DescribeInstances",
```

```
                "ec2:DescribeInstanceTypes"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "tag:GetTagKeys",
                "tag:GetTagValues",
                "tag:GetResources"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "storagegateway:DescribeCachediSCSIVolumes",
                "storagegateway:DescribeStorediSCSIVolumes"
            ],
            "Resource": "arn:aws:storagegateway:*:*:gateway/*/volume/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "storagegateway:ListGateways"
            ],
            "Resource": "arn:aws:storagegateway:*:*:*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "storagegateway:DescribeGatewayInformation",
                "storagegateway:ListVolumes",
                "storagegateway:ListLocalDisks"
            ],
            "Resource": "arn:aws:storagegateway:*:*:gateway/*"
        },
        {
            "Action": [
                "iam:ListRoles",
                "iam:GetRole"
            ],
            "Effect": "Allow",
```

```
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "organizations:DescribeOrganization",
            "Resource": "*"
        },
        {
            "Action": "fsx:DescribeBackups",
            "Effect": "Allow",
            "Resource": "arn:aws:fsx:*:*:backup/*"
        },
        {
            "Action": "fsx:DescribeFileSystems",
            "Effect": "Allow",
            "Resource": "arn:aws:fsx:*:*:file-system/*"
        },
        {
            "Action": "ds:DescribeDirectories",
            "Effect": "Allow",
            "Resource": "*"
        },
        {
          "Sid": "AmsChangeRecordKMSPolicy",
          "Effect": "Allow",
          "Action": [
            "kms:Encrypt",
            "kms:Decrypt",
            "kms:GenerateDataKey"
          ],
          "Resource": [
            "arn:aws:kms:${AWS::Region}:${AWS::AccountId}:key/*"
          ],
          "Condition": {
            "ForAnyValue:StringLike": {
              "kms:ResourceAliases": "alias/AMSCloudTrailLogManagement"
            }
          }
        },
        {
          "Sid": "AmsChangeRecordAthenaReadPolicy",
          "Effect": "Allow",
          "Action": [
            "athena:BatchGetNamedQuery",
```

```
            "athena:Get*",
            "athena:List*",
            "athena:StartQueryExecution",
            "athena:UpdateWorkGroup",
            "glue:GetDatabase*",
            "glue:GetTable*",
            "s3:GetAccountPublicAccessBlock",
            "s3:ListAccessPoints",
            "s3:ListAllMyBuckets"
          ],
          "Resource": "*"
        },
        {
          "Sid": "AmsChangeRecordS3ReadPolicy",
          "Effect": "Allow",
          "Action": [
            "s3:Get*",
            "s3:List*"
          ],
          "Resource": [
            "arn:aws:s3:::ams-a${AWS::AccountId}-athena-results-${AWS::Region}",
            "arn:aws:s3:::ams-a${AWS::AccountId}-athena-results-${AWS::Region}/*",
            "arn:aws:s3:::ams-a${AWS::AccountId}-cloudtrail-${AWS::Region}",
            "arn:aws:s3:::ams-a${AWS::AccountId}-cloudtrail-${AWS::Region}/*"
          ]
        },
        {
          "Sid": "AmsChangeRecordS3WritePolicy",
          "Effect": "Allow",
          "Action": [
            "s3:PutObject",
            "s3:PutObjectLegalHold",
            "s3:PutObjectRetention"
          ],
          "Resource": [
            "arn:aws:s3:::ams-a${AWS::AccountId}-athena-results-${AWS::Region}/*"
          ]
        },
        {
          "Sid": "MaciePolicy",
          "Effect": "Allow",
          "Action": [
            "macie2:GetFindingStatistics"
          ],
```

```
            "Resource": "*"
          },
          {
            "Sid": "GuardDutyReadPolicy",
            "Effect": "Allow",
            "Action": [
              "guardduty:GetFindingsStatistics",
              "guardduty:ListDetectors"
            ],
            "Resource": "*"
          },
          {
            "Sid": "SupportReadPolicy",
            "Effect": "Allow",
            "Action": "support:Describe*",
            "Resource": "*"
          },
          {
            "Sid": "ConfigReadPolicy",
            "Effect": "Allow",
            "Action": [
              "config:Get*",
              "config:Describe*",
              "config:List*"
            ],
            "Resource": "*"
          },
          {
            "Sid": "AppConfigReadPolicy",
            "Effect": "Allow",
            "Action": [
              "appconfig:List*",
              "appconfig:Get*"
            ],
            "Resource": "*"
          },
          {
            "Sid": "CloudFormationReadPolicy",
            "Effect": "Allow",
            "Action": [
              "cloudformation:DescribeStacks"
            ],
            "Resource": "*"
          },
```

```
            {
              "Sid": "EC2ReadPolicy",
              "Effect": "Allow",
              "Action": [
                "ec2:DescribeInstances"
              ],
              "Resource": "*"
            },
            {
              "Sid": "SSMReadPolicy",
              "Effect": "Allow",
              "Action": [
                "ssm:Describe*",
                "ssm:Get*",
                "ssm:List*"
              ],
              "Resource": "*"
            },
            {
              "Sid": "TagReadPolicy",
              "Effect": "Allow",
              "Action": [
                "tag:GetResources",
                "tag:GetTagKeys"
              ],
              "Resource": "*"
            },
            {
              "Sid": "CloudtrailReadPolicy",
              "Effect": "Allow",
              "Action": [
                "cloudtrail:DescribeTrails",
                "cloudtrail:GetTrailStatus",
                "cloudtrail:LookupEvents"
              ],
              "Resource": "*"
            },
            {
              "Sid": "EventBridgePolicy",
              "Effect": "Allow",
              "Action": [
                "events:Describe*",
                "events:List*",
                "events:TestEventPattern"
```

```
            ],
            "Resource": "*"
          }
        ]
      }
```

Perché e quando AMS accede al tuo account

Gli operatori di AMS Accelerate (Accelerate) possono accedere alla console e alle istanze del vostro account, in determinate circostanze, per gestire le vostre risorse. Questi eventi di accesso sono documentati nei tuoi AWS CloudTrail (CloudTrail) log. Per i dettagli su come esaminare l'attività del tuo account da parte del team di AMS Accelerate Operations e di AMS Accelerate automation, consulta. Monitoraggio delle modifiche nei tuoi account AMS Accelerate

Nei seguenti argomenti vengono spiegati perché, quando e come AMS accede al tuo account.

Trigger di accesso all'account cliente AMS

L'attività di accesso all'account cliente AMS è determinata dai trigger. I fattori scatenanti oggi sono i AWS ticket creati nel nostro sistema di gestione dei problemi in risposta agli allarmi e agli eventi di Amazon CloudWatch (CloudWatch) e le segnalazioni di incidenti o le richieste di assistenza che invii. Per ogni accesso potrebbero essere eseguite più chiamate di servizio e attività a livello di host.

La giustificazione dell'accesso, i trigger e l'iniziatore del trigger sono elencati nella tabella seguente.

Trigger di accesso

Accesso	Iniziatore	Trigger
Applicazione delle patch	AMS	Problema con la patch
Indagine interna sui problemi	ARMS	Problema (un problema che è stato identificato come sistemico)
Indagine e risoluzione degli avvisi	AMS	Elementi di lavoro operativi (SSM OpsItems) di AWS Systems Manager

Accesso	Iniziatore	Trigger
Indagine e risoluzione degli incidenti	Utente corrente	Caso di assistenza in entrata (un incidente o una richiesta di assistenza inviata dall'utente)
Adempimento della richiesta di assistenza in entrata	Utente corrente	

Ruoli IAM di accesso all'account cliente AMS

Gli operatori AMS richiedono i seguenti ruoli per gestire il tuo account.

> **Note**
>
> I ruoli di accesso AMS consentono agli operatori AMS di accedere alle risorse dell'utente per fornire funzionalità AMS (vediDescrizione del servizio). La modifica di questi ruoli può inibire la nostra capacità di fornire tali funzionalità. Se hai bisogno di modificare i ruoli di accesso AMS, consulta il tuo Cloud Architect.

Ruoli IAM per l'accesso di AMS agli account dei clienti

Nome ruolo	Description
ams-access-admin	Questo ruolo ha pieno accesso amministrativo al tuo account senza restrizioni. I servizi AMS utilizzano questo ruolo con politiche di sessione restrittive che limitano l'accesso all'implementazione dell'infrastruttura AMS e alla gestione dell'account.
ams-access-admin-operations	Questo ruolo concede agli operatori AMS le autorizzazioni amministrative per gestire l'account. Questo ruolo non concede autorizzazioni di lettura, scrittura o eliminazione ai contenuti dei clienti in AWS servizi comunemente usati come archivi dati, come Amazon Simple Storage Service, Amazon Relational Database Service, Amazon DynamoDB, Amazon Redshift e Amazon. ElastiCache Solo gli operatori AMS qualifica

Nome ruolo	Description
	ti che hanno una solida conoscenza ed esperienza nella gestione degli accessi possono assumere questo ruolo. Questi operatori fungono da punto di riferimento per i problemi di gestione degli accessi e accedono ai vostri account per risolvere i problemi di accesso degli operatori AMS.
ams-access-management	Implementato manualmente durante l'onboarding. Il sistema AMS Access richiede questo ruolo per la gestione `ams-access-roles` e lo stack. `ams-access-managed-policies`
ams-access-operations	Questo ruolo dispone delle autorizzazioni per eseguire attività amministrative nei tuoi account. Questo ruolo non dispone delle autorizzazioni di lettura, scrittura o eliminazione dei contenuti dei clienti nei AWS servizi comunemente usati come archivi dati, come Amazon Simple Storage Service, Amazon Relational Database Service, Amazon DynamoDB, Amazon Redshift e Amazon. ElastiCache Anche le autorizzazioni per eseguire operazioni di AWS Identity and Access Management scrittura sono escluse da questo ruolo. Lo staff operativo di AMS Accelerate e gli architetti cloud (CAs) possono assumere questo ruolo.
ams-access-read-only	Questo ruolo ha accesso in sola lettura al tuo account. Lo staff operativo di AMS Accelerate e gli architett i cloud (CAs) possono assumere questo ruolo. Le autorizzazioni di lettura per i contenuti dei clienti nei AWS servizi comunemente utilizzati come archivi dati, come Amazon S3, Amazon RDS, DynamoDB, Amazon Redshift, e questo ruolo non viene concesso ElastiCac he.

Nome ruolo	Description
ams-access-security-analyst	Questo ruolo di sicurezza AMS dispone delle autorizza zioni nel tuo account AMS per eseguire il monitorag gio dedicato degli avvisi di sicurezza e la gestione degli incidenti di sicurezza. Solo pochissime persone selezionate di AMS Security possono assumere questo ruolo.
ams-access-security-analyst-sola lettura	Questo ruolo di sicurezza AMS è limitato alle autorizza zioni di sola lettura nel tuo account AMS per eseguire il monitoraggio dedicato degli avvisi di sicurezza e la gestione degli incidenti di sicurezza.

> **Note**
>
> Questo è il modello per il ruolo. ams-access-management È lo stack che gli architetti cloud (CAs) distribuiscono manualmente nel tuo account al momento dell'onboarding: management-role.yaml.
> Questo è il modello per i diversi ruoli di accesso per i diversi livelli di accesso:,,,: accelerate-roles.json. ams-access-read-only ams-access-operations ams-access-admin-operations ams-access-admin

In che modo AMS accede al tuo account

Gli operatori di AMS Accelerate possono accedere alla console e alle istanze del tuo account, in determinate circostanze.

Gli operatori AMS utilizzano il servizio di accesso interno AMS Accelerate per accedere ai vostri account in modo sicuro e controllato. Per accedere alle istanze, gli operatori AMS utilizzano lo stesso servizio di accesso AMS interno del broker e, una volta concesso l'accesso, gli operatori AMS Accelerate utilizzano il gestore di sessioni SSM per ottenere l'accesso utilizzando le credenziali di sessione. L'accesso RDP per le istanze Windows viene fornito stabilendo il port forwarding all'istanza e creando un utente locale tramite SSM. Le credenziali utente locali vengono utilizzate per l'accesso RDP e rimosse alla fine della sessione.

Come e quando usare l'account utente root in AMS

L'utente root è il superutente del tuo AWS account. AMS monitora l'utilizzo dei root. Ti consigliamo di utilizzare root solo per le poche attività che lo richiedono, ad esempio: modifica delle impostazioni dell'account, attivazione dell'accesso AWS Identity and Access Management (IAM) alla fatturazione e alla gestione dei costi, modifica della password root e abilitazione dell'autenticazione a più fattori (MFA). Vedi Attività che richiedono credenziali utente root nella Guida per l'utente.AWS Identity and Access Management

Root con AMS Accelerate:

AMS non ti proibisce di utilizzare il tuo account utente root. Tuttavia, AMS Operations and Security considera il suo utilizzo come un problema su cui indagare e contatteremo il tuo team di sicurezza per ogni utilizzo.

Ti consigliamo di contattare il CSDM e la CA con ventiquattro ore di anticipo, per informarli sulle operazioni di accesso root che intendi eseguire.

Operazioni AMS e risposta di sicurezza all'utilizzo del root:

AMS riceve un allarme quando viene utilizzato l'account utente root. Se l'utilizzo delle credenziali root non è pianificato, contatta il team di sicurezza AMS e il team dell'account per verificare se si tratta di un'attività prevista. Se non si tratta di un'attività prevista, AMS collabora con il team di sicurezza per esaminare il problema.

Gestione della sicurezza in AMS Accelerate

AWS Managed Services utilizza più controlli per proteggere le tue risorse informative e aiutarti a mantenere sicura la tua AWS infrastruttura. AMS Accelerate gestisce una libreria di Regole di AWS Config azioni correttive per garantire che tutti gli account siano conformi agli standard di settore per la sicurezza e l'integrità operativa. Regole di AWS Config monitora continuamente la modifica della configurazione tra le risorse registrate. Se una modifica viola una delle condizioni delle regole, AMS ne segnala i risultati e consente di porre rimedio alle violazioni automaticamente o su richiesta, in base alla gravità della violazione. Regole di AWS Config facilitare la conformità agli standard stabiliti da: il Center for Internet Security (CIS), il National Institute of Standards and Technology (NIST) Cloud Security Framework (CSF), l'Health Insurance Portability and Accountability Act (HIPAA) e il Payment Card Industry (PCI) Data Security Standard (DSS).

Inoltre, AMS sfrutta Amazon GuardDuty per identificare attività potenzialmente non autorizzate o dannose nel tuo AWS ambiente. AMS monitora GuardDuty i risultati 24 ore su 24, 7 giorni su 7. AMS collabora con voi per comprendere l'impatto dei risultati e identificare le misure correttive sulla base delle raccomandazioni delle migliori pratiche. AMS utilizza anche Amazon Macie per proteggere i tuoi dati sensibili come informazioni sanitarie personali (PHI), informazioni di identificazione personale (PII) e dati finanziari.

> **Note**
>
> Amazon Macie è un servizio opzionale e non è abilitato per impostazione predefinita.

AMS Accelerate offre una gamma di servizi operativi per aiutarti a raggiungere l'eccellenza operativa su AWS. Per saperne di più su come AMS aiuta i team a raggiungere l'eccellenza operativa complessiva Cloud AWS grazie alle principali funzionalità operative di AMS, tra cui l'helpdesk 24 ore su 24, 7 giorni su 7, il monitoraggio proattivo, la sicurezza, l'applicazione di patch, la registrazione e la registrazione, consulta i diagrammi dell'architettura di riferimento di AMS.

Argomenti

- Usa il documento SSM Log4j per scoprire le occorrenze in Accelerate
- Monitoraggio della sicurezza dell'infrastruttura in AMS
- Protezione dei dati in Accelerate
- AWS Identity and Access Management in AMS Accelerate

- Risposta agli incidenti di sicurezza in AMS
- Registrazione e monitoraggio degli eventi di sicurezza in Accelerate
- Conformità della configurazione in Acceler
- Risposta agli incidenti in Accelerate
- Resilienza nell'accelerazione
- Controllo di sicurezza per sistemi end-of-support operativi
- Le migliori pratiche di sicurezza in Accelerate
- Revisioni di sicurezza delle richieste di modifica
- Domande frequenti sulla sicurezza

Usa il documento SSM Log4j per scoprire le occorrenze in Accelerate

Il documento Log4j (AWS Systems Manager documento SSM) consente di cercare la libreria Apache Log4j2 all'interno dei carichi di lavoro inseriti. Il documento di automazione fornisce un rapporto sull'ID di processo delle applicazioni Java in cui è attiva la libreria Log4j2.

Il rapporto include informazioni sugli archivi Java (file JAR), che si trovano all'interno dell'ambiente specificato che contiene la classe. JndiLookup È consigliabile aggiornare le librerie scoperte all'ultima versione disponibile. Questo aggiornamento mitiga la Remote Code Execution (RCE) identificata tramite CVE-2021-44228. Scarica l'ultima versione della libreria Log4j da Apache. Per ulteriori informazioni, consulta Scaricare Apache Log4j 2.

Il documento è condiviso con tutte le regioni che hanno aderito ad Accelerate,. Per accedere al documento, completa i seguenti passaggi:

1. Apri la AWS Systems Manager console all'indirizzo https://console.aws.amazon.com/systems-manager/.
2. Nel riquadro di navigazione, scegli Documenti.
3. Scegli Condiviso con me.
4. Nella casella di ricerca, inserisci AWSManagedServices-GatherLog4jInformation.
5. Usa il controllo della velocità per eseguire il documento su larga scala.

Il documento AWSManagedServices-GatherLog 4JInformation raccoglie i seguenti parametri:

- InstanceId: (Obbligatorio) ID dell'istanza. EC2
- S3Bucket: (Facoltativo) L'URL prefirmato S3 o l'URI S3 (s3://BUCKET_NAME) su cui caricare i risultati.
- AutomationAssumeRole: (Obbligatorio) L'ARN del ruolo che consente all'automazione di eseguire azioni per tuo conto.

È consigliabile eseguire questo documento utilizzando il controllo della frequenza. È possibile impostare il parametro di controllo della InstanceIdvelocità su e assegnargli un elenco di istanze oppure applicare una combinazione tag-chiave per individuare tutte le EC2 istanze che hanno un determinato tag. AWS Managed Services consiglia inoltre di fornire un bucket Amazon Simple Storage Service (Amazon S3) su cui caricare i risultati, in modo da poter creare un report dai dati archiviati in S3. Per un esempio di come aggregare i risultati in S3, consulta EC2 Instance Stack | Gather Log4j Information.

Se non riesci ad aggiornare il pacchetto, segui le linee guida delineate da AWS Sicurezza in Utilizzare AWS i servizi di sicurezza per proteggere, rilevare e rispondere alla vulnerabilità di Log4j. Per mitigare le vulnerabilità rimuovendo la funzionalità della JndiLookup classe, esegui l'hot patch Log4j in linea con le tue applicazioni Java. Per ulteriori informazioni sull'hot patch, consulta Hotpatch for Apache Log4j.

Per domande sull'output dell'automazione o su come procedere con ulteriori mitigazioni, invia una richiesta di assistenza.

Monitoraggio della sicurezza dell'infrastruttura in AMS

Quando effettui l' AWS onboarding su AMS Accelerate e implementa la seguente infrastruttura di AWS Config base e il seguente set di regole, AMS Accelerate utilizza queste regole per monitorare i tuoi account.

- AWS Config ruolo collegato al servizio: AMS Accelerate implementa il ruolo collegato al servizio denominato AWSServiceRoleForConfig, che viene utilizzato da AWS Config per interrogare lo stato di altri servizi. AWS Il ruolo AWSServiceRoleForConfigcollegato al servizio si fida che il servizio assuma il ruolo. AWS Config La politica di autorizzazione per il AWSServiceRoleForConfigruolo contiene autorizzazioni di sola lettura e di sola scrittura per le risorse e autorizzazioni di sola lettura per le AWS Config risorse di altri servizi che supportano. AWS Config Se hai già un ruolo configurato con AWS Config Recorder, AMS Accelerate verifica che al ruolo esistente sia associata

una policy gestita di AWS Config. In caso contrario, AMS Accelerate sostituisce il ruolo con il ruolo collegato al servizio. AWSServiceRoleForConfig

- AWS Config registratore e canale di distribuzione: AWS Config utilizza il registratore di configurazione per rilevare le modifiche nelle configurazioni delle risorse e acquisirle come elementi di configurazione. AMS Accelerate implementa il registratore di configurazione in tutti i servizi Regioni AWS, con registrazione continua di tutte le risorse. AMS Accelerate crea anche il canale di distribuzione della configurazione, un bucket Amazon S3, che viene utilizzato per registrare le modifiche che si verificano nelle risorse. AWS Il registratore di configurazione aggiorna gli stati di configurazione tramite il canale di distribuzione. Il registratore di configurazione e il canale di consegna sono necessari per funzionare. AWS Config AMS Accelerate crea il registratore in tutto Regioni AWS e un canale di distribuzione in un unico canale. Regione AWS Se hai già un registratore e un canale di distribuzione in un canale Regione AWS, AMS Accelerate non elimina le AWS Config risorse esistenti, ma AMS Accelerate utilizza il registratore e il canale di consegna esistenti dopo aver verificato che siano configurati correttamente. Per ulteriori informazioni su come ridurre AWS Config i costi, consulta. Ridurre i AWS Config costi in Accelerate
- AWS Config regole: AMS Accelerate mantiene una libreria di Regole di AWS Config azioni correttive per aiutarvi a rispettare gli standard di settore per la sicurezza e l'integrità operativa. Regole di AWS Config monitora continuamente le modifiche alla configurazione tra le risorse registrate. Se una modifica viola una delle condizioni delle regole, AMS ne segnala i risultati e consente di porre rimedio alle violazioni automaticamente o su richiesta, in base alla gravità della violazione. Regole di AWS Config facilitare la conformità agli standard stabiliti da: il Center for Internet Security (CIS), il National Institute of Standards and Technology (NIST) Cloud Security Framework (CSF), l'Health Insurance Portability and Accountability Act (HIPAA) e il Payment Card Industry (PCI) Data Security Standard (DSS).
- AWS Config autorizzazione dell'aggregatore: un aggregatore è un tipo di AWS Config risorsa che raccoglie AWS Config dati di configurazione e conformità da più account e più regioni. AMS Accelerate inserisce il tuo account in un aggregatore di configurazione dal quale AMS Accelerate aggrega le informazioni sulla configurazione delle risorse e i dati di conformità della configurazione dell'account e genera il rapporto di conformità. Se nell'account di proprietà di AMS sono configurati degli aggregatori esistenti, AMS Accelerate implementa un aggregatore aggiuntivo e l'aggregatore esistente non viene modificato.

> **Note**
>
> L'aggregatore Config non è configurato nei tuoi account, ma negli account di proprietà di AMS e i tuoi account vengono inseriti in esso.

Per saperne di più, consulta: AWS Config

- AWS Config: Che cos'è Config?
- Regole di AWS Config: Valutazione delle risorse con regole
- Regole di AWS Config: Controllo dinamico della conformità: Regole di AWS Config — Controllo dinamico della conformità per le risorse cloud
- AWS Config Aggregatore: aggregazione di dati multiaccount e più regioni

Per informazioni sui report, vedere. AWS Config Rapporto di controllo della conformità

Utilizzo di ruoli collegati ai servizi per AMS Accelerate

AMS Accelerate utilizza AWS Identity and Access Management ruoli collegati ai servizi (IAM). Un ruolo collegato al servizio (SLR) è un tipo unico di ruolo IAM collegato direttamente ad AMS Accelerate. I ruoli collegati ai servizi sono predefiniti da AMS Accelerate e includono tutte le autorizzazioni richieste dal servizio per chiamare altri servizi per tuo conto. AWS

Un ruolo collegato ai servizi semplifica la configurazione di AMS Accelerate perché non è necessario aggiungere manualmente le autorizzazioni necessarie. AMS Accelerate definisce le autorizzazioni dei suoi ruoli collegati ai servizi e, se non diversamente definito, solo AMS Accelerate può assumerne i ruoli. Le autorizzazioni definite includono la policy di attendibilità e la policy delle autorizzazioni. Una policy delle autorizzazioni specifica non può essere collegata a un'altra entità IAM.

Per informazioni su altri servizi che supportano i ruoli collegati ai servizi, consulta i AWS servizi che funzionano con IAM e cerca i servizi con Sì nella colonna Ruoli collegati ai servizi. Scegliere Sì in corrispondenza di un link per visualizzare la documentazione relativa al ruolo collegato al servizio per tale servizio.

Ruolo collegato ai servizi del toolkit di implementazione per AMS Accelerate

AMS Accelerate utilizza il cosiddetto ruolo collegato ai servizi (SLR), che implementa l'infrastruttura AWSServiceRoleForAWSManagedServicesDeploymentToolkitAMS Accelerate negli account dei clienti.

> **Note**
>
> Questa politica è stata aggiornata di recente; per i dettagli, consulta. Accelera gli aggiornamenti ai ruoli collegati ai servizi

Toolkit di implementazione AMS Accelerate SLR

Il ruolo AWSService RoleFor AWSManaged ServicesDeploymentToolkit collegato al servizio prevede che i seguenti servizi assumano il ruolo:

- `deploymenttoolkit.managedservices.amazonaws.com`

La policy denominata AWSManagedServicesDeploymentToolkitPolicyconsente ad AMS Accelerate di eseguire azioni sulle seguenti risorse:

- `arn:aws*:s3:::ams-cdktoolkit*`
- `arn:aws*:cloudformation:*:*:stack/ams-cdk-toolkit*`
- `arn:aws:ecr:*:*:repository/ams-cdktoolkit*`

Questa reflex concede ad Amazon S3 le autorizzazioni per creare e gestire il bucket di distribuzione utilizzato da AMS per caricare risorse, come CloudFormation modelli o pacchetti di risorse Lambda, nell'account per le distribuzioni dei componenti. Questa reflex concede CloudFormation le autorizzazioni per distribuire lo stack che definisce i bucket di distribuzione. CloudFormation Per i dettagli o per scaricare la policy, consulta. AWSManagedServices_DeploymentToolkitPolicy

Per consentire a un'entità IAM (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato al servizio è necessario configurare le relative autorizzazioni. Per ulteriori informazioni, consulta le autorizzazioni dei ruoli collegati ai servizi nella Guida per l'utente IAM.

Creazione di un toolkit di implementazione SLR per AMS Accelerate

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Quando effettui l'onboarding su AMS tramite Console di gestione AWS, la o l' AWS API AWS CLI, AMS Accelerate crea automaticamente il ruolo collegato al servizio.

> **Important**
>
> Questo ruolo collegato al servizio può apparire nel tuo account se utilizzavi il servizio AMS Accelerate prima del 09 giugno 2022, quando ha iniziato a supportare i ruoli collegati ai servizi, quindi AMS Accelerate ha creato il ruolo nel tuo account. AWSService RoleFor AWSManaged ServicesDeploymentToolkit Per ulteriori informazioni, consulta Un nuovo ruolo è apparso nel mio account IAM.

Se elimini questo ruolo collegato al servizio, è possibile ricrearlo seguendo lo stesso processo utilizzato per ricreare il ruolo nell'account. Quando effettui l'accesso ad AMS, AMS Accelerate crea nuovamente il ruolo collegato al servizio per te.

Modifica di un toolkit di implementazione SLR per AMS Accelerate

AMS Accelerate non consente di modificare il ruolo collegato al AWSService RoleFor AWSManaged ServicesDeploymentToolkit servizio. Dopo avere creato un ruolo collegato al servizio, non sarà possibile modificarne il nome perché varie entità potrebbero farvi riferimento. È possibile tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta Modifica di un ruolo collegato al servizio nella Guida per l'utente di IAM.

Eliminazione di un toolkit di implementazione SLR per AMS Accelerate

Non è necessario eliminare manualmente il ruolo. AWSService RoleFor AWSManaged ServicesDeploymentToolkit Quando esci da AMS tramite Console di gestione AWS, the o l' AWS API AWS CLI, AMS Accelerate ripulisce le risorse ed elimina automaticamente il ruolo collegato al servizio.

Puoi anche utilizzare la console IAM, AWS CLI o l' AWS API per eliminare manualmente il ruolo collegato al servizio. Per farlo, sarà necessario prima eseguire manualmente la pulizia delle risorse associate al ruolo collegato ai servizi e poi eliminarlo manualmente.

> **Note**
>
> Se il servizio AMS Accelerate utilizza il ruolo quando si tenta di eliminare le risorse, l'eliminazione potrebbe non riuscire. In questo caso, attendi alcuni minuti e quindi ripeti l'operazione.

Per eliminare le risorse AMS Accelerate utilizzate dal ruolo AWSService RoleFor AWSManaged ServicesDeploymentToolkit collegato al servizio

Elimina `ams-cdk-toolkit` lo stack da tutte le regioni in cui è stato effettuato l'onboarding del tuo account in AMS (potresti dover prima svuotare manualmente i bucket S3).

Per eliminare manualmente il ruolo collegato ai servizi mediante IAM

Utilizza la console IAM AWS CLI, o l' AWS API per eliminare il ruolo collegato al servizio. AWSService RoleFor AWSManaged ServicesDeploymentToolkit Per ulteriori informazioni, consulta Eliminazione di un ruolo collegato al servizio nella Guida per l'utente IAM.

Detective controlla il ruolo collegato ai servizi per AMS Accelerate

AMS Accelerate utilizza il ruolo collegato ai servizi (SLR) denominato AWSServiceRoleForManagedServices_DetectiveControlsConfig: AWS Managed Services utilizza questo ruolo collegato ai servizi per distribuire config-recorder, regole di configurazione e controlli di rilevamento dei bucket S3.

Al ruolo collegato al servizio è associata la seguente politica gestita: _. AWSServiceRoleForManagedServices_DetectiveControlsConfigAWSManagedServices_DetectiveControlsC
Per gli aggiornamenti a questa policy, consulta Accelera gli aggiornamenti delle policy AWS gestite.

Autorizzazioni per i controlli investigativi SLR for AMS Accelerate

Il ruolo AWSServiceRoleForManagedServices_DetectiveControlsConfig collegato al servizio prevede che i seguenti servizi assumano il ruolo:

- `detectivecontrols.managedservices.amazonaws.com`

A questo ruolo è associata la policy `AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy` AWS gestita (vedi AWS politica gestita: _ AWSManagedServices_DetectiveControlsConfig ServiceRolePolicy
Il servizio utilizza il ruolo per creare e configurare AMS Detective Controls nel tuo account), che richiede l'implementazione di risorse come bucket s3, regole di configurazione e un aggregatore. È necessario configurare le autorizzazioni per consentire a un'entità IAM (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato al servizio. Per ulteriori informazioni, vedere Service-Linked Role Permissions nella AWS Identity and Access Management User Guide.

Creazione di un Detective Controls SLR per AMS Accelerate

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Quando effettui l'accesso ad AMS tramite Console di gestione AWS, la o l' AWS API AWS CLI, AMS Accelerate crea automaticamente il ruolo collegato al servizio.

> **Important**
>
> Questo ruolo collegato al servizio può apparire nel tuo account se utilizzavi il servizio AMS Accelerate prima del 09 giugno 2022, quando ha iniziato a supportare ruoli collegati ai servizi, allora AMS Accelerate ha creato il ruolo nel tuo account.

AWSServiceRoleForManagedServices_DetectiveControlsConfig Per ulteriori informazioni, consulta Un nuovo ruolo è apparso nel mio account IAM.

Se elimini questo ruolo collegato al servizio, è possibile ricrearlo seguendo lo stesso processo utilizzato per ricreare il ruolo nell'account. Quando effettui l'accesso ad AMS, AMS Accelerate crea nuovamente il ruolo collegato al servizio per te.

Modifica di una reflex di Detective Controls per AMS Accelerate

AMS Accelerate non consente di modificare il ruolo collegato al AWSServiceRoleForManagedServices_DetectiveControlsConfig servizio. Dopo avere creato un ruolo collegato al servizio, non sarà possibile modificarne il nome perché varie entità potrebbero farvi riferimento. È possibile tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta Modifica di un ruolo collegato al servizio nella Guida per l'utente IAM.

Eliminazione di un Detective Controls SLR per AMS Accelerate

Non è necessario eliminare manualmente il AWSServiceRoleForManagedServices_DetectiveControlsConfig ruolo. Quando esci da AMS tramite Console di gestione AWS, the o l' AWS API AWS CLI, AMS Accelerate ripulisce le risorse ed elimina automaticamente il ruolo collegato al servizio.

Puoi anche utilizzare la console IAM, AWS CLI o l' AWS API per eliminare manualmente il ruolo collegato al servizio. Per farlo, sarà necessario prima eseguire manualmente la pulizia delle risorse associate al ruolo collegato ai servizi e poi eliminarlo manualmente.

> **Note**
>
> Se il servizio AMS Accelerate utilizza il ruolo quando si tenta di eliminare le risorse, l'eliminazione potrebbe non riuscire. In questo caso, attendi alcuni minuti e quindi ripeti l'operazione.

Per eliminare le risorse AMS Accelerate utilizzate dal ruolo AWSServiceRoleForManagedServices_DetectiveControlsConfig collegato al servizio

Elimina `ams-detective-controls-config-recorder` `ams-detective-controls-config-rules-cdk` e `ams-detective-controls-infrastructure-cdk` accumula pile da tutte le

regioni in cui il tuo account è stato registrato in AMS (potresti dover prima svuotare manualmente i bucket S3).

Per eliminare manualmente il ruolo collegato ai servizi mediante IAM

Usa la console IAM AWS CLI, o l' AWS API per eliminare il ruolo collegato al servizio. AWSServiceRoleForManagedServices_DetectiveControlsConfig Per ulteriori informazioni, consulta Eliminazione del ruolo collegato ai servizi nella Guida per l'utente IAM.

Amazon EventBridge regola il ruolo collegato ai servizi per AMS Accelerate

AMS Accelerate utilizza il ruolo collegato al servizio (SLR) denominato. AWSServiceRoleForManagedServices_Events Questo ruolo si affida a uno dei responsabili del servizio AWS Managed Services (events.managedservices.amazonaws.com) affinché assuma il ruolo per te. Il servizio utilizza il ruolo per creare una regola EventBridge gestita da Amazon. Questa regola è l'infrastruttura richiesta nel tuo account AWS per fornire informazioni sulla modifica dello stato di allarme dal tuo account ad AWS Managed Services.

Autorizzazioni per EventBridge SLR for AMS Accelerate

Il ruolo AWSServiceRoleForManagedServices_Events collegato al servizio prevede che i seguenti servizi assumano il ruolo:

- `events.managedservices.amazonaws.com`

A questo ruolo è associata la politica `AWSManagedServices_EventsServiceRolePolicy` AWS gestita (vedi). AWS politica gestita: AWSManagedServices_EventsServiceRolePolicy Il servizio utilizza il ruolo per fornire informazioni sulla modifica dello stato di allarme dall'account dell'utente ad AMS. Per consentire a un'entità IAM (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato al servizio è necessario configurare le relative autorizzazioni. Per ulteriori informazioni, consulta Autorizzazioni del ruolo collegato ai servizi nella Guida per l'utente di AWS Identity and Access Management .

Puoi scaricare il file JSON AWSManagedServices_EventsServiceRolePolicy in questo ZIP: EventsServiceRolePolicy.zip.

Creazione di una EventBridge reflex per AMS Accelerate

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Quando effettui l'accesso ad AMS tramite Console di gestione AWS, la o l' AWS API AWS CLI, AMS Accelerate crea automaticamente il ruolo collegato ai servizi.

> **Important**
>
> Questo ruolo legato al servizio può apparire nel tuo account se utilizzavi il servizio AMS Accelerate prima del 7 febbraio 2023, quando ha iniziato a supportare i ruoli collegati ai servizi, quindi AMS Accelerate ha creato il ruolo nel tuo account. AWSServiceRoleForManagedServices_Events Per ulteriori informazioni, consulta Un nuovo ruolo è apparso nel mio account IAM.

Se elimini questo ruolo collegato al servizio, è possibile ricrearlo seguendo lo stesso processo utilizzato per ricreare il ruolo nell'account. Quando accedi ad AMS, AMS Accelerate crea nuovamente il ruolo collegato ai servizi per te.

Modificare una EventBridge reflex per AMS Accelerate

AMS Accelerate non consente di modificare il ruolo collegato al AWSServiceRoleForManagedServices_Events servizio. Dopo avere creato un ruolo collegato al servizio, non sarà possibile modificarne il nome perché varie entità potrebbero farvi riferimento. È possibile tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta Modifica di un ruolo collegato al servizio nella Guida per l'utente di IAM.

Eliminazione di una EventBridge reflex per AMS Accelerate

Non è necessario eliminare manualmente il AWSServiceRoleForManagedServices_Events ruolo. Quando esci da AMS tramite Console di gestione AWS, the o l' AWS API AWS CLI, AMS Accelerate ripulisce le risorse ed elimina automaticamente il ruolo collegato al servizio.

Puoi anche utilizzare la console IAM, AWS CLI o l' AWS API per eliminare manualmente il ruolo collegato al servizio. Per farlo, sarà necessario prima eseguire manualmente la pulizia delle risorse associate al ruolo collegato ai servizi e poi eliminarlo manualmente.

> **Note**
>
> Se il servizio AMS Accelerate utilizza il ruolo quando si tenta di eliminare le risorse, l'eliminazione potrebbe non riuscire. In questo caso, attendi alcuni minuti e quindi ripeti l'operazione.

Per eliminare le risorse AMS Accelerate utilizzate dal ruolo AWSServiceRoleForManagedServices_Events collegato al servizio

Per eliminare manualmente il ruolo collegato ai servizi mediante IAM

Utilizza la console IAM AWS CLI, l'o l' AWS API per eliminare il ruolo collegato al AWSServiceRoleForManagedServices_Events servizio. Per ulteriori informazioni, consulta Eliminazione del ruolo collegato ai servizi nella Guida per l'utente IAM.

Contatta il ruolo collegato al servizio per AMS Accelerate

AMS Accelerate utilizza il ruolo collegato al servizio (SLR) denominato AWSServiceRoleForManagedServices_Contacts: questo ruolo facilita le notifiche automatiche in caso di incidenti, consentendo al servizio di leggere i tag esistenti della risorsa interessata e recuperare l'e-mail configurata del punto di contatto appropriato.

Questo è l'unico servizio che utilizza questo ruolo collegato al servizio.

Al ruolo AWSServiceRoleForManagedServices_Contactscollegato al servizio è allegata la seguente politica gestita:. AWSManagedServices_ContactsServiceRolePolicy Per gli aggiornamenti a questa policy, consulta Accelera gli aggiornamenti delle policy AWS gestite.

Autorizzazioni per Contacts SLR for AMS Accelerate

Il ruolo AWSServiceRoleForManagedServices_Contacts collegato al servizio prevede che i seguenti servizi assumano il ruolo:

- `contacts-service.managedservices.amazonaws.com`

A questo ruolo è associata la policy gestita da `AWSManagedServices_ContactsServiceRolePolicy` AWS (vediAWS politica gestita: AWSManagedServices_ContactsServiceRolePolicy). Il servizio utilizza il ruolo per leggere i tag su qualsiasi AWS risorsa e trovare l'e-mail contenuta nel tag, del punto di contatto appropriato

per quando si verificano incidenti. Questo ruolo facilita le notifiche automatiche in caso di incidenti consentendo ad AMS di leggere quel tag su una risorsa interessata e recuperare l'e-mail. Per ulteriori informazioni, vedere Service-Linked Role Permissions nella AWS Identity and Access Management User Guide.

> **Important**
>
> Non memorizzare informazioni personali identificabili o altre informazioni riservate o sensibili nei tag. AMS utilizza i tag per fornirti servizi di amministrazione. I tag non sono destinati ad essere utilizzati per dati privati o sensibili.

La politica di autorizzazione dei ruoli denominata AWSManagedServices_ContactsServiceRolePolicy consente ad AMS Accelerate di completare le seguenti azioni sulle risorse specificate:

- Azione: consente al servizio Contatti di leggere i tag specificamente configurati per contenere l'e-mail a cui AMS invia notifiche di incidenti su qualsiasi risorsa AWS.

Puoi scaricare il file JSON AWSManagedServices_ContactsServiceRolePolicy in questo ZIP: ContactsServicePolicy.zip.

Creazione di una SLR con contatti per AMS Accelerate

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Quando effettui l'onboarding su AMS tramite Console di gestione AWS, la o l' AWS API AWS CLI, AMS Accelerate crea automaticamente il ruolo collegato al servizio.

> **Important**
>
> Questo ruolo legato al servizio può apparire nel tuo account se utilizzavi il servizio AMS Accelerate prima del 16 febbraio 2023, quando ha iniziato a supportare i ruoli collegati ai servizi e quindi AMS Accelerate ha creato il ruolo nel tuo account. AWSServiceRoleForManagedServices_Contacts Per ulteriori informazioni, consulta Un nuovo ruolo è apparso nel mio account IAM.

Se elimini questo ruolo collegato al servizio, è possibile ricrearlo seguendo lo stesso processo utilizzato per ricreare il ruolo nell'account. Quando accedi ad AMS, AMS Accelerate crea nuovamente il ruolo collegato ai servizi per te.

Modifica di un Contacts SLR per AMS Accelerate

AMS Accelerate non consente di modificare il ruolo collegato al AWSServiceRoleForManagedServices_Contacts servizio. Dopo avere creato un ruolo collegato al servizio, non sarà possibile modificarne il nome perché varie entità potrebbero farvi riferimento. È possibile tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta Modifica di un ruolo collegato al servizio nella Guida per l'utente di IAM.

Eliminazione di un Contacts SLR per AMS Accelerate

Non è necessario eliminare manualmente il AWSServiceRoleForManagedServices_Contacts ruolo. Quando esci da AMS tramite Console di gestione AWS, the o l' AWS API AWS CLI, AMS Accelerate ripulisce le risorse ed elimina automaticamente il ruolo collegato al servizio.

Puoi anche utilizzare la console IAM, AWS CLI o l' AWS API per eliminare manualmente il ruolo collegato al servizio. Per farlo, sarà necessario prima eseguire manualmente la pulizia delle risorse associate al ruolo collegato ai servizi e poi eliminarlo manualmente.

> **Note**
>
> Se il servizio AMS Accelerate utilizza il ruolo quando si tenta di eliminare le risorse, l'eliminazione potrebbe non riuscire. In questo caso, attendi alcuni minuti e quindi ripeti l'operazione.

Per eliminare le risorse AMS Accelerate utilizzate dal ruolo AWSServiceRoleForManagedServices_Contacts collegato al servizio

Per eliminare manualmente il ruolo collegato ai servizi mediante IAM

Utilizza la console IAM AWS CLI, l'o l' AWS API per eliminare il ruolo collegato al AWSServiceRoleForManagedServices_Contacts servizio. Per ulteriori informazioni, consulta Eliminazione del ruolo collegato ai servizi nella Guida per l'utente IAM.

Regioni supportate per i ruoli collegati ai servizi di AMS Accelerate

AMS Accelerate supporta l'utilizzo di ruoli collegati al servizio in tutte le regioni in cui il servizio è disponibile. Per ulteriori informazioni, consulta Regioni ed endpoint di AWS.

Accelera gli aggiornamenti ai ruoli collegati ai servizi

Visualizza i dettagli sugli aggiornamenti ai ruoli collegati al servizio Accelerate da quando questo servizio ha iniziato a tenere traccia di queste modifiche. Per ricevere avvisi automatici sulle modifiche a questa pagina, iscriviti al feed RSS nella pagina Accelerate. Guida per l'utente della cronologia dei documenti di AMS Accelerate

Modifica	Descrizione	Data

Politica aggiornata — Deployment Toolkit	• Queste nuove autorizzazioni sono state aggiunte per la risorsa: `arn:aws:ecr:*:*:repository/ams-cdktoolkit*`
	`ecr:BatchGetRepositoryScanningConfiguration`
	`ecr:PutImageScanningConfiguration`
		4 aprile 2024

Politica aggiornata — Deployment Toolkit	• Queste nuove autorizzazioni sono state aggiunte per la risorsa: `arn:aws:cloudformation:*:*:stack/ams-cdk-toolkit*`
	`cloudformation:DeleteChangeSet`
	`cloudformation:DescribeStackEvents`
	`cloudformation:GetTemplate`
	`cloudformation:TagResource`
	`cloudformation:UntagResource`
	• Queste nuove autorizzazioni sono state aggiunte per la risorsa: `arn:aws:ecr:*:*:repository/ams-cdktoolkit*`
	`ecr:CreateRepository`
	`ecr:DeleteLifecyclePolicy`
	`ecr:DeleteRepository`
	`ecr:DeleteRepositoryPolicy`
	`ecr:DescribeRepositories`
	`ecr:GetLifecyclePolicy`
	`ecr:ListTagsForResource`
	`ecr:PutImageTagMutability`
	`ecr:PutLifecyclePolicy`
		09 maggio 2023

Modifica	Descrizione	Data

	<pre>ecr:SetRepositoryPolicy
	ecr:TagResource
	ecr:UntagResource</pre>
	• Inoltre, alcune azioni esistenti con caratteri jolly erano limitate a singole azioni:
	<pre>- s3:DeleteObject*
	+ s3:DeleteObject
	+ s3:DeleteObjectTagging
	+ s3:DeleteObjectVersion
	+ s3:DeleteObjectVersionTagging
	
	- s3:GetObject*
	+ s3:GetObject
	+ s3:GetObjectAcl
	+ s3:GetObjectAttributes
	+ s3:GetObjectLegalHold
	+ s3:GetObjectRetention
	+ s3:GetObjectTagging
	+ s3:GetObjectVersion
	+ s3:GetObjectVersionAcl
	+ s3:GetObjectVersionAttributes
	+ s3:GetObjectVersionForReplication
	+ s3:GetObjectVersionTagging
	+ s3:GetObjectVersionTorrent
	
	- cloudformation:UpdateTermination*
	+ cloudformation:UpdateTerminationProt
	ection</pre>	

Politica aggiornata — Detective Controls	• Le CloudFormation azioni sono state ulteriormente analizzate dopo la conferma con il team di sicurezza e accesso • Le azioni Lambda sono state rimosse dalla policy in quanto non influiscono sull'imbarco onboarding/off	10 aprile 2023

Modifica	Descrizione	Data
Politica aggiornata — Detective Controls	È stata aggiornata la politica e aggiunta la politica sui limiti delle autorizzazioni.	21 marzo 2023
Nuovo ruolo collegato al servizio: Contacts SLR	Accelerate ha aggiunto un nuovo ruolo collegato al servizio Contatti. Questo ruolo facilita le notifiche automatiche in caso di incidenti consentendo al servizio di leggere i tag esistenti della risorsa interessata e recuperare l'e-mail configurata del punto di contatto appropriato.	16 febbraio 2023
Nuovo ruolo collegato al servizio: EventBridge	Accelerate ha aggiunto un nuovo ruolo collegato ai servizi per una regola Amazon EventBridge . Questo ruolo si affida a uno dei responsabili del servizio AWS Managed Services (events.managedservices.amazonaws.com) affinché assuma il ruolo per te. Il servizio utilizza il ruolo per creare una regola EventBridge gestita da Amazon. Questa regola è l'infrastruttura richiesta nel tuo account AWS per fornire informazioni sulla modifica dello stato di allarme dal tuo account ad AWS Managed Services.	7 febbraio 2023

Ruolo aggiornato collegato al servizio — Deployment Toolkit	Accelera l'aggiornamento AWSService RoleFor AWSManaged ServicesDeploymentToolkit con nuove autorizzazioni S3.
	
	Sono state aggiunte queste nuove autorizzazioni:
	
	`"s3:GetLifecycleConfiguration",`
	`"s3:GetBucketLogging",`
	`"s3:ListBucket",`
	`"s3:GetBucketVersioning",`
	`"s3:PutLifecycleConfiguration",`
	`"s3:GetBucketLocation",`
	`"s3:GetObject*"`
		30 gennaio 2023

Modifica	Descrizione	Data
Accelera, inizia a tracciare le modifiche	Accelerate ha iniziato a tracciare le modifiche per i ruoli collegati ai servizi.	30 novembre 2022
Nuovo ruolo legato ai servizi: Detective Controls	Accelerate ha aggiunto un nuovo ruolo collegato al servizio per implementare Accelerate Detective Controls. AWS Managed Services utilizza questo ruolo collegato ai servizi per distribuire config-recorder, regole di configura zione e controlli di rilevamento dei bucket S3.	13 ottobre 2022
Nuovo ruolo collegato ai servizi: Deployment Toolkit	Accelerate ha aggiunto un nuovo ruolo collegato ai servizi per implementare l'infrastruttura Accelerate. questo ruolo implementa l'infrastruttura AMS Accelerate negli account dei clienti.	09 giugno 2022

AWS politiche gestite per AMS Accelerate

Una politica AWS gestita è una politica autonoma creata e amministrata da AWS. AWS le politiche gestite sono progettate per fornire autorizzazioni per molti casi d'uso comuni, in modo da poter iniziare ad assegnare autorizzazioni a utenti, gruppi e ruoli.

Tieni presente che le policy AWS gestite potrebbero non concedere le autorizzazioni con il privilegio minimo per i tuoi casi d'uso specifici, poiché sono disponibili per tutti i clienti. AWS Ti consigliamo pertanto di ridurre ulteriormente le autorizzazioni definendo policy gestite dal cliente specifiche per i tuoi casi d'uso.

Non è possibile modificare le autorizzazioni definite nelle politiche gestite. AWS Se AWS aggiorna le autorizzazioni definite in una politica AWS gestita, l'aggiornamento ha effetto su tutte le identità principali (utenti, gruppi e ruoli) a cui è associata la politica. AWS è più probabile che aggiorni una policy AWS gestita quando ne Servizio AWS viene lanciata una nuova o quando diventano disponibili nuove operazioni API per i servizi esistenti.

Per ulteriori informazioni, consultare Policy gestite da AWSnella Guida per l'utente di IAM.

Per una tabella delle modifiche, vedereAccelera gli aggiornamenti delle policy AWS gestite.

AWS politica gestita: AWSManagedServices_AlarmManagerPermissionsBoundary

AWS Managed Services (AMS) utilizza la politica `AWSManagedServices_AlarmManagerPermissionsBoundary` AWS gestita. Questa politica AWS gestita viene utilizzata in AWSManagedServices_AlarmManager _ ServiceRolePolicy per limitare le autorizzazioni dei ruoli IAM creati da. AWSServiceRoleForManagedServices_AlarmManager

Questa policy concede ai ruoli IAM creati come parte diCome funziona Alarm Manager, le autorizzazioni per eseguire operazioni come la AWS valutazione di Config, la lettura di AWS Config per recuperare la configurazione di Alarm Manager e la creazione degli allarmi Amazon necessari. CloudWatch

La `AWSManagedServices_AlarmManagerPermissionsBoundary` policy è allegata al ruolo collegato al servizio. `AWSServiceRoleForManagedServices_DetectiveControlsConfig` Per gli aggiornamenti a questo ruolo, consulta. Accelera gli aggiornamenti ai ruoli collegati ai servizi

Puoi allegare questa policy alle tue identità IAM.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `AWS Config`— Consente le autorizzazioni per valutare le regole di configurazione e selezionare la configurazione delle risorse.
- `AWS AppConfig`— Consente le autorizzazioni per recuperare la configurazione. AlarmManager
- `Amazon S3`— Consente le autorizzazioni per utilizzare AlarmManager bucket e oggetti.
- `Amazon CloudWatch`— Consente le autorizzazioni per leggere e inserire allarmi e AlarmManager metriche gestiti.
- `AWS Resource Groups and Tags`— Consente le autorizzazioni per leggere i tag delle risorse.
- `Amazon EC2`— Consente le autorizzazioni per leggere le EC2 risorse di Amazon.
- `Amazon Redshift`— Consente le autorizzazioni per leggere le istanze e i cluster Redshift.
- `Amazon FSx`— Consente le autorizzazioni per descrivere file system, volumi e tag di risorse.
- `Amazon CloudWatch Synthetics`— Consente le autorizzazioni per leggere le risorse Synthetics.
- `Amazon Elastic Kubernetes Service`— Consente le autorizzazioni per descrivere il cluster Amazon EKS.

- `Amazon ElastiCache`— Consente le autorizzazioni per descrivere le risorse.

È possibile scaricare il file di policy in questo file ZIP: RecommendedPermissionBoundary.zip.

AWS politica gestita: _ AWSManagedServices_DetectiveControlsConfig ServiceRolePolicy

AWS Managed Services (AMS) utilizza la politica `AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy` AWS gestita. Questa politica AWS gestita è allegata al ruolo `AWSServiceRoleForManagedServices_DetectiveControlsConfig` collegato al servizio (vedi). Detective controlla il ruolo collegato ai servizi per AMS Accelerate Per gli aggiornamenti al ruolo collegato al `AWSServiceRoleForManagedServices_DetectiveControlsConfig` servizio, consulta. Accelera gli aggiornamenti ai ruoli collegati ai servizi

La policy consente al ruolo collegato al servizio di completare le azioni al posto tuo.

Puoi allegare la ServiceRolePolicy policy AWSManagedServices_DetectiveControlsConfig _ alle tue entità IAM.

Per ulteriori informazioni, consulta Utilizzo di ruoli collegati ai servizi per AMS Accelerate.

Dettagli dell'autorizzazione

Questa politica dispone delle seguenti autorizzazioni per consentire a AWS Managed Services Detective Controls di distribuire e configurare tutte le risorse necessarie.

- `CloudFormation`— Consente ad AMS Detective Controls di implementare CloudFormation stack con risorse come bucket s3, regole di configurazione e config-recorder.
- `AWS Config`— Consente ad AMS Detective Controls di creare regole di configurazione AMS, configurare un aggregatore e taggare le risorse.
- `Amazon S3`— consente ad AMS Detective Controls di gestire i suoi bucket s3.

Puoi scaricare il file di policy JSON in questo ZIP: DetectiveControlsConfig _ .zip. ServiceRolePolicy

AWS politica gestita: AWSManaged ServicesDeploymentToolkitPolicy

AWS Managed Services (AMS) utilizza la politica `AWSManagedServicesDeploymentToolkitPolicy` AWS gestita. Questa politica AWS gestita è

allegata al ruolo `AWSServiceRoleForAWSManagedServicesDeploymentToolkit` collegato al servizio (vedi). Ruolo collegato ai servizi del toolkit di implementazione per AMS Accelerate La policy consente al ruolo collegato al servizio di completare le azioni al posto tuo. Non è possibile attribuire questa policy alle entità IAM. Per ulteriori informazioni, consulta Utilizzo di ruoli collegati ai servizi per AMS Accelerate.

Per gli aggiornamenti al ruolo `AWSServiceRoleForManagedServicesDeploymentToolkitPolicy` collegato al servizio, consulta. Accelera gli aggiornamenti ai ruoli collegati ai servizi

Dettagli dell'autorizzazione

Questa politica dispone delle seguenti autorizzazioni per consentire a AWS Managed Services Detective Controls di distribuire e configurare tutte le risorse necessarie.

- `CloudFormation`— Consente ad AMS Deployment Toolkit di implementare stack CFN con le risorse S3 richieste da CDK.
- `Amazon S3`— consente ad AMS Deployment Toolkit di gestire i propri bucket S3.
- `Elastic Container Registry`— consente ad AMS Deployment Toolkit di gestire il proprio repository ECR utilizzato per distribuire le risorse necessarie alle app AMS CDK.

Puoi scaricare il file di policy JSON in questo ZIP: .zip. AWSManaged ServicesDeploymentToolkitPolicy

AWS politica gestita: AWSManagedServices_EventsServiceRolePolicy

AWS Managed Services (AMS) utilizza la policy gestita da `AWSManagedServices_EventsServiceRolePolicy` AWS. Questa policy AWS gestita è allegata al ruolo collegato al `AWSServiceRoleForManagedServices_Events`servizio. La policy consente al ruolo collegato al servizio di completare le azioni al posto tuo. Non è possibile attribuire questa policy alle entità IAM. Per ulteriori informazioni, consulta Utilizzo di ruoli collegati ai servizi per AMS Accelerate.

Per gli aggiornamenti al ruolo `AWSServiceRoleForManagedServices_Events` collegato al servizio, consulta. Accelera gli aggiornamenti ai ruoli collegati ai servizi

Dettagli dell'autorizzazione

Questa policy dispone delle seguenti autorizzazioni per consentire ad Amazon di EventBridge fornire informazioni sulla modifica dello stato di allarme dal tuo account ad AWS Managed Services.

- `events`— Consente ad Accelerate di creare regole EventBridge gestite da Amazon. Questa regola è l'infrastruttura necessaria Account AWS per fornire informazioni sulla modifica dello stato di allarme dal tuo account a AWS Managed Services.

Puoi scaricare il file di policy JSON in questo ZIP: EventsServiceRolePolicy.zip.

AWS politica gestita: AWSManagedServices_ContactsServiceRolePolicy

AWS Managed Services (AMS) utilizza la policy gestita da `AWSManagedServices_ContactsServiceRolePolicy` AWS. Questa policy AWS gestita è allegata al ruolo `AWSServiceRoleForManagedServices_Contacts` collegato al servizio (vedi). Creazione di una SLR con contatti per AMS Accelerate La policy consente ad AMS Contacts SLR di esaminare i tag delle risorse e i relativi valori sulle risorse AWS. Non è possibile attribuire questa policy alle entità IAM. Per ulteriori informazioni, consulta Utilizzo di ruoli collegati ai servizi per AMS Accelerate.

> **Important**
>
> Non memorizzare informazioni personali identificabili o altre informazioni riservate o sensibili nei tag. AMS utilizza i tag per fornirti servizi di amministrazione. I tag non sono destinati ad essere utilizzati per dati privati o sensibili.

Per gli aggiornamenti al ruolo `AWSServiceRoleForManagedServices_Contacts` collegato al servizio, consulta. Accelera gli aggiornamenti ai ruoli collegati ai servizi

Dettagli dell'autorizzazione

Questo criterio dispone delle seguenti autorizzazioni per consentire a Contacts SLR di leggere i tag delle risorse per recuperare le informazioni di contatto delle risorse che avete impostato in precedenza.

- `IAM`— Consente al servizio Contacts di esaminare i tag sui ruoli IAM e sugli utenti IAM.
- `Amazon EC2`— Consente al servizio Contatti di visualizzare i tag nelle EC2 risorse Amazon.
- `Amazon S3`— Consente a Contacts Service di esaminare i tag sui bucket Amazon S3. Questa azione utilizza una condizione per garantire che AMS acceda ai tag bucket utilizzando l'intestazione HTTP Authorization, utilizzando il protocollo di firma SigV4 e utilizzando HTTPS con

TLS 1.2 o versione successiva. Per ulteriori informazioni, consulta Metodi di autenticazione e chiavi di policy specifiche per l'autenticazione di Amazon S3 Signature versione 4.

- `Tag`— Consente al servizio Contatti di visualizzare i tag su altre AWS risorse.

- «iam: ListRoleTags «, «iam: ListUserTags «, «tag: GetResources «, «tag: GetTagKeys «, «tag: GetTagValues «, «ec2: DescribeTags «, «s3:» GetBucketTagging

Puoi scaricare il file di policy JSON in questo ZIP: .zip. ContactsServicePolicy

Accelera gli aggiornamenti delle policy AWS gestite

Visualizza i dettagli sugli aggiornamenti delle politiche AWS gestite per Accelerate da quando questo servizio ha iniziato a tenere traccia di queste modifiche.

Modifica	Descrizione	Data

Politica aggiornata — Deployment Toolkit	• Queste nuove autorizzazioni sono state aggiunte per la risorsa: `arn:aws:ecr:*:*:repository/ams-cdktoolkit*`
	`ecr:BatchGetRepositoryScanningConfiguration`
	`ecr:PutImageScanningConfiguration`
		4 aprile 2024

Politica aggiornata — Deployment Toolkit	• Queste nuove autorizzazioni sono state aggiunte per la risorsa: `arn:aws:cloudformation:*:*:stack/ams-cdk-toolkit*`
	`cloudformation:DeleteChangeSet`
	`cloudformation:DescribeStackEvents`
	`cloudformation:GetTemplate`
	`cloudformation:TagResource`
	`cloudformation:UntagResource`
	• Queste nuove autorizzazioni sono state aggiunte per la risorsa: `arn:aws:ecr:*:*:repository/ams-cdktoolkit*`
		9 maggio 2023

Modifica	Descrizione	Data

	<pre>ecr:CreateRepository
	
	ecr:DeleteLifecyclePolicy
	ecr:DeleteRepository
	ecr:DeleteRepositoryPolicy
	ecr:DescribeRepositories
	ecr:GetLifecyclePolicy
	ecr:ListTagsForResource
	ecr:PutImageTagMutability
	ecr:PutLifecyclePolicy
	ecr:SetRepositoryPolicy
	ecr:TagResource
	ecr:UntagResource</pre> • Inoltre, alcune azioni esistenti con caratteri jolly erano limitate a singole azioni:
	<pre>- s3:DeleteObject*
	
	+ s3:DeleteObject
	+ s3:DeleteObjectTagging
	+ s3:DeleteObjectVersion
	+ s3:DeleteObjectVersionTagging
	
	- s3:GetObject*
	+ s3:GetObject
	+ s3:GetObjectAcl
	+ s3:GetObjectAttributes
	+ s3:GetObjectLegalHold
	+ s3:GetObjectRetention
	+ s3:GetObjectTagging
	+ s3:GetObjectVersion
	+ s3:GetObjectVersionAcl
	+ s3:GetObjectVersionAttributes
	+ s3:GetObjectVersionForReplication
	+ s3:GetObjectVersionTagging
	+ s3:GetObjectVersionTorrent
	
	- cloudformation:UpdateTermination*</pre>	

Modifica	Descrizione	Data
	`+ cloudformation:UpdateTerminationProtection`	
Politica aggiornata — Detective Controls	• Le CloudFormation azioni sono state ulteriormente analizzate dopo la conferma con il team di sicurezza e accesso • Le azioni Lambda sono state rimosse dalla policy in quanto non influiscono sull'imbarco onboarding/off	10 aprile 2023
Politica aggiornata — Detective Controls	`L'ListAttachedRolePolicies` azione viene rimossa dalla politica. L'azione aveva Resource come jolly (*). Poiché «list» è un'azione non mutativa, le viene dato accesso a tutte le risorse e il jolly non è consentito.	28 marzo 2023
Politica aggiornata — Detective Controls	Aggiornato il criterio e aggiunto il criterio sui limiti delle autorizzazioni.	21 marzo 2023
Nuova politica: Contacts Service	Accelerate ha aggiunto una nuova politica per esaminare le informazioni di contatto del tuo account nei tag delle risorse. Accelerate ha aggiunto una nuova politica per leggere i tag delle risorse in modo da poter recuperare le informazioni di contatto delle risorse che avete impostato in precedenza.	16 febbraio 2023
Nuova politica: Events Service	Accelerate ha aggiunto una nuova policy per fornire informazioni sulla modifica dello stato di allarme dal tuo account ad AWS Managed Services. Concede i ruoli IAM creati come parte delle Come funziona Alarm Manager autorizzazioni per creare una regola EventBridge gestita Amazon richiesta.	07 febbraio 2023

Modifica	Descrizione	Data
Politica aggiornata — Deployment Toolkit	Sono state aggiunte le autorizzazioni S3 per supportare l'offboarding dei clienti da Accelerate.	30 gennaio 2023
Nuova politica — Detective Controls	Consente al ruolo collegato al servizio di completare le azioni necessarie all'implementazione di Accelerate detective Controls. Detective controlla il ruolo collegato ai servizi per AMS Accelerate	19 dicembre 2022
Nuova politica: Alarm Manager	Accelerate ha aggiunto una nuova politica per consentire le autorizzazioni per eseguire attività di gestione degli allarmi. Concede i ruoli IAM creati come parte delle Come funziona Alarm Manager autorizzazioni per eseguire operazioni come la AWS valutazione di Config, la lettura di AWS Config per la configurazione del gestore degli allarmi, la creazione degli allarmi Amazon necessari. CloudWatch	30 novembre 2022
Accelera, inizia a tracciare le modifiche	Accelerate ha iniziato a tracciare le modifiche per le sue politiche AWS gestite.	30 novembre 2022
Nuova politica: Deployment Toolkit	Accelerate ha aggiunto questa politica per le attività di distribuzione. Concede ai ruoli collegati al servizio le AWSServiceRoleForAWSManagedServicesDeploymentToolkitautorizzazioni per accedere e aggiornare i bucket e gli stack Amazon S3 relativi alla distribuzione. CloudFormation	09 giugno 2022

Protezione dei dati in Accelerate

AMS Accelerate sfrutta strumenti e processi nativi Servizi AWS come Amazon GuardDuty, Amazon Macie (opzionalmente) e altri strumenti e processi proprietari interni per monitorare continuamente gli account gestiti. Dopo l'attivazione di un allarme, AMS Accelerate si assume la responsabilità della valutazione iniziale e della risposta all'allarme. I processi di risposta AMS si basano sugli standard NIST. AMS Accelerate testa regolarmente i processi di risposta utilizzando Security Incident Response Simulation per allineare il flusso di lavoro con i programmi di risposta alla sicurezza dei clienti esistenti.

Quando AMS Accelerate rileva una violazione, o una minaccia imminente di violazione, delle vostre politiche di AWS sicurezza, Accelerate raccoglie informazioni, comprese le risorse interessate e qualsiasi modifica relativa alla configurazione. AMS Accelerate fornisce follow-the-sun supporto 24 ore su 24, 7 giorni su 7, 365 giorni all'anno con operatori dedicati che esaminano e esaminano attivamente le dashboard di monitoraggio, le code di incidenti e le richieste di assistenza su tutti gli account gestiti. Accelerate analizza i risultati con esperti di sicurezza interni per analizzare l'attività e inviarti notifiche tramite i contatti relativi all'escalation di sicurezza elencati nel tuo account.

Sulla base dei risultati, Accelerate interagisce con te in modo proattivo. Se ritieni che l'attività non sia autorizzata o sospetta, AMS collabora con te per indagare e risolvere o contenere il problema. Esistono alcuni tipi di risultati generati da Accelerate GuardDuty che richiedono la conferma dell'impatto prima che Accelerate intraprenda qualsiasi azione. Ad esempio, il tipo di GuardDuty risultato UnauthorizedAccess:IAMUser/ConsoleLogininindica che uno dei tuoi utenti ha effettuato l'accesso da una posizione insolita; AMS ti avvisa e ti chiede di esaminare i risultati per confermare se questo comportamento è legittimo.

Monitoraggio con Amazon Macie

> **Important**
>
> AMS Accelerate non supporta il monitoraggio con Amazon Macie nella regione Asia Pacifico (Malesia).

AMS Accelerate supporta, ed è una best practice utilizzare, Amazon Macie per rilevare un elenco ampio e completo di dati sensibili, come informazioni sanitarie personali (PHI), informazioni di identificazione personale (PII) e dati finanziari.

Puoi configurare Macie per l'esecuzione periodica su qualsiasi bucket Amazon S3. Ciò automatizza la valutazione di oggetti nuovi o modificati all'interno di un bucket nel tempo. Man mano che vengono generati i risultati di sicurezza, AMS invia una notifica all'utente e collabora con l'utente per porvi rimedio, se necessario.

Per ulteriori informazioni, consulta Analizzare i risultati di Amazon Macie.

Monitora con GuardDuty

GuardDuty è un servizio di monitoraggio continuo della sicurezza che utilizza feed di intelligence sulle minacce, come elenchi di indirizzi IP e domini dannosi, e l'apprendimento automatico per identificare attività impreviste, potenzialmente non autorizzate e dannose all'interno dell'ambiente. AWS Ciò potrebbe includere problemi come l'aumento dei privilegi, l'uso di credenziali esposte o la comunicazione con indirizzi IP o domini dannosi. GuardDuty monitora il comportamento di Account AWS accesso alla ricerca di segnali di compromissione, come installazioni di infrastrutture non autorizzate, istanze distribuite in una regione che non hai mai usato. AWS GuardDuty rileva anche chiamate API insolite, ad esempio una modifica delle politiche relative alle password per ridurre la sicurezza delle password. Per ulteriori informazioni, consulta la Guida per l'utente GuardDuty .

Per visualizzare e analizzare i GuardDuty risultati, completa i seguenti passaggi:

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
2. Scegli Risultati, quindi seleziona un risultato specifico per visualizzarne i dettagli. I dettagli di ogni risultato variano a seconda del tipo di scoperta, delle risorse coinvolte e della natura dell'attività.

Per ulteriori informazioni sui campi di ricerca disponibili, vedere i dettagli dei GuardDuty risultati.

Utilizza le regole di GuardDuty soppressione per filtrare i risultati

Una regola di soppressione è un insieme di criteri costituito da un attributo di filtro associato a un valore. È possibile utilizzare le regole di soppressione per filtrare i risultati di basso valore su cui non si intende agire, ad esempio risultati falsi positivi o attività note. Il filtraggio dei risultati aiuta a riconoscere più facilmente le minacce alla sicurezza che potrebbero avere il maggiore impatto sull'ambiente.

Per filtrare i risultati, le regole di soppressione archiviano automaticamente i nuovi risultati che corrispondono ai criteri specificati. I risultati archiviati non vengono inviati a AWS Security Hub, Amazon S3 o Events. CloudTrail Pertanto, i filtri di soppressione riducono i dati non utilizzabili se si

utilizzano i risultati tramite GuardDuty Security Hub o un'applicazione di avvisi e ticketing SIEM di terze parti.

AMS dispone di una serie definita di criteri per identificare le regole di soppressione per gli account gestiti. Quando un account gestito soddisfa questi criteri, AMS applica i filtri e crea una richiesta di servizio (SR) che descrive in dettaglio il filtro di soppressione distribuito.

È possibile comunicare con AMS tramite un SR per modificare o ripristinare i filtri di soppressione.

Visualizza i risultati archiviati

GuardDuty continua a generare risultati anche quando tali risultati corrispondono alle tue regole di soppressione. I risultati soppressi vengono contrassegnati come archiviati. GuardDuty archivia i risultati archiviati per 90 giorni. È possibile visualizzare i risultati archiviati nella GuardDuty console per quei 90 giorni selezionando Archiviati dalla tabella dei risultati. Oppure, visualizza i risultati archiviati tramite l' GuardDuty API utilizzando l'ListFindingsAPI con un findingCriteria di service.archived uguale a true.

Casi d'uso comuni per le regole di soppressione

I seguenti tipi di risultati presentano casi d'uso comuni per l'applicazione delle regole di soppressione.

- recon:EC2/PortScan: utilizza una regola di soppressione per archiviare automaticamente i risultati quando si utilizza uno scanner di vulnerabilità autorizzato.
- UnauthorizedAccessrecon:EC2/PortScanSSHBrute: Usa una regola di soppressione per archiviare automaticamente i risultati quando usi uno scanner di vulnerabilità autorizzato. ----sep----:EC2/ Force: usa una regola di soppressione per archiviare automaticamente i risultati quando sono indirizzati a istanze bastion.
- ReCon:EC2/ PortProbeUnprotectedPort: Utilizza una regola di soppressione per archiviare automaticamente i risultati quando sono indirizzati a istanze esposte intenzionalmente.

Monitoraggio con il firewall DNS di Amazon Route 53 Resolver

Amazon Route 53 Resolver risponde in modo ricorsivo alle richieste DNS provenienti da risorse AWS per record pubblici, nomi DNS specifici di Amazon VPC e zone ospitate private di Amazon Route 53 ed è disponibile per impostazione predefinita in tutti. VPCs Con il DNS Firewall per Route 53 Resolver è possibile filtrare e regolare il traffico DNS in uscita per il proprio cloud privato virtuale. A tale scopo, è possibile creare raccolte riutilizzabili di regole di filtro nei gruppi di regole di DNS Firewall, associare i gruppi di regole al VPC e quindi monitorare l'attività nei record e nei parametri

di DNS Firewall. In base all'attività, è possibile regolare di conseguenza il comportamento di DNS Firewall. Per ulteriori informazioni, consulta Usare DNS Firewall per filtrare il traffico DNS in uscita.

Per visualizzare e gestire la configurazione del firewall DNS di Route 53 Resolver, utilizzare la seguente procedura:

1. Accedi Console di gestione AWS e apri la console Amazon VPC all'indirizzo. https://console.aws.amazon.com/vpc/
2. In DNS Firewall, scegli Gruppi di regole.
3. Rivedi, modifica o elimina la configurazione esistente o crea un nuovo gruppo di regole. Per ulteriori informazioni, consulta Come funziona Route 53 Resolver DNS Firewall.

Monitoraggio e sicurezza del firewall DNS di Amazon Route 53 Resolver

Amazon Route 53 DNS Firewall utilizza i concetti di associazione di regole, azione delle regole e priorità di valutazione delle regole. Un elenco di domini è un insieme riutilizzabile di specifiche di dominio utilizzate in una regola DNS Firewall all'interno di un gruppo di regole. Quando associ un gruppo di regole a un VPC, DNS Firewall confronta le query DNS con gli elenchi di dominio utilizzati nelle regole. Se DNS Firewall trova una corrispondenza, gestisce la query DNS in base all'azione della regola corrispondente. Per ulteriori informazioni sui gruppi di regole e sulle regole, consulta Gruppi di regole e regole del firewall DNS.

Gli elenchi di domini rientrano in due categorie principali:

- Elenchi di domini gestiti, che AWS creano e gestiscono per te.
- Elenchi di domini personalizzati, creati e gestiti dall'utente.

I gruppi di regole vengono valutati in base all'indice di priorità delle associazioni.

Per impostazione predefinita, AMS implementa una configurazione di base costituita dalle seguenti regole e gruppi di regole:

- Un gruppo di regole denominato. `DefaultSecurityMonitoringRule` Il gruppo di regole ha la massima priorità di associazione disponibile al momento della creazione per ogni VPC esistente in ogni VPC abilitato. Regione AWS
- Una regola denominata `DefaultSecurityMonitoringRule` con priorità 1 all'interno del gruppo di `DefaultSecurityMonitoringRule` regole, utilizzando l'elenco dei domini `AWSManagedDomainsAggregateThreatList` gestiti con l'azione ALERT.

Se si dispone di una configurazione esistente, la configurazione di base viene distribuita con una priorità inferiore rispetto alla configurazione esistente. La configurazione esistente è quella predefinita. La configurazione di base di AMS viene utilizzata come soluzione generica se la configurazione esistente non fornisce istruzioni con priorità più elevata su come gestire la risoluzione delle query. Per modificare o rimuovere la configurazione di base, esegui una delle seguenti operazioni:

- Contatta il tuo Cloud Service Delivery Manager (CSDM) o Cloud Architect (CA).
- Crea una richiesta di servizio.

La crittografia dei dati in AMS Accelerate

AMS Accelerate ne utilizza diversi Servizi AWS per la crittografia dei dati.

Amazon Simple Storage Service offre diverse opzioni di crittografia degli oggetti che proteggono i dati in transito e a riposo. La crittografia lato server crittografa l'oggetto prima di salvarlo su disco nei suoi data center e quindi lo decrittografa al momento del download. Se la richiesta è autenticata e sono disponibili le autorizzazioni per l'accesso, non c'è differenza nelle modalità di accesso agli oggetti, crittografati o meno. Per ulteriori informazioni, consulta Protezione dei dati in Amazon S3.

AWS Identity and Access Management in AMS Accelerate

AWS Identity and Access Management è un servizio web che consente di controllare in modo sicuro l'accesso alle AWS risorse. Utilizza IAM per controllare chi è autenticato (accesso effettuato) e autorizzato (dispone di autorizzazioni) per l'utilizzo di risorse. Durante l'onboarding di AMS Accelerate, sei responsabile della creazione di ruoli di amministratore IAM su più account all'interno di ciascuno dei tuoi account gestiti.

In AMS Accelerate, sei responsabile della gestione dell'accesso alle tue Account AWS e alle relative risorse sottostanti, come le soluzioni di gestione degli accessi, le politiche di accesso e i processi correlati. Ciò significa che gestisci il ciclo di vita degli utenti, le autorizzazioni nei servizi di directory e il sistema di autenticazione federato, per accedere alla console o. AWS AWS APIs Per aiutarti a gestire la tua soluzione di accesso, AMS Accelerate implementa AWS Config regole che rilevano le configurazioni errate più comuni di IAM e fornisce notifiche di correzione. Per ulteriori informazioni, consulta Regole gestite di AWS Config.

Autenticazione con identità in AMS Accelerate

AMS utilizza i ruoli IAM, che sono un tipo di identità IAM. Un ruolo IAM è simile a quello di un utente, in quanto è un'identità con politiche di autorizzazione che determinano ciò che l'identità può e non può fare. AWS Tuttavia, a un ruolo non sono associate credenziali e, invece di essere associato in modo univoco a una persona, è assunto da chiunque ne abbia bisogno. Un utente IAM può assumere un ruolo per ottenere temporaneamente autorizzazioni diverse per un'attività specifica.

I ruoli di accesso sono controllati dall'appartenenza al gruppo interno, che viene amministrata e rivista periodicamente da Operations Management. AMS utilizza i seguenti ruoli IAM.

> **Note**
>
> I ruoli di accesso AMS consentono agli operatori AMS di accedere alle risorse dell'utente per fornire funzionalità AMS (vediDescrizione del servizio). La modifica di questi ruoli può inibire la nostra capacità di fornire tali funzionalità. Se hai bisogno di modificare i ruoli di accesso AMS, consulta il tuo Cloud Architect.

Role name (Nome ruolo)	Descrizione
Utilizzato da (entità): solo AMS Access Service	
ams-access-management	Implementato manualmente dall'utente durante l'onboarding. Assunto solo da AMS Access per implementare o aggiornare i ruoli di accesso. Rimane nel tuo account dopo l'onboarding per eventuali aggiornamenti futuri dei ruoli di accesso.
Utilizzato da (entità): AMS Operations	
ams-access-admin-operations	Questo ruolo dispone delle autorizzazioni amministrative per operare negli account, ma non dispone delle autorizzazioni per leggere, scrivere o eliminare i contenuti dei clienti nei AWS servizi comunemente usati come archivi dati, come Amazon Simple Storage

Role name (Nome ruolo)	Descrizione
	Service, Amazon Relational Database Service, Amazon DynamoDB, Amazon Redshift e Amazon. ElastiCache Solo pochissime persone selezionate di AMS possono assumere questo ruolo.
ams-access-operations	Questo ruolo AMS Operations dispone delle autorizzazioni per eseguire attività amministr ative nei tuoi account. Questo ruolo non dispone delle autorizzazioni di lettura, scrittura o eliminazione dei contenuti dei clienti nei AWS servizi comunemente usati come archivi dati, come Amazon Simple Storage Service, Amazon Relational Database Service, Amazon DynamoDB, Amazon Redshift e Amazon. ElastiCache Anche le autorizzazioni per eseguire operazioni di AWS Identity and Access Management scrittura sono escluse da questo ruolo.
ams-access-read-only	Questo ruolo di sola lettura AMS è limitato alle autorizzazioni di sola lettura nel tuo account AMS. Le autorizzazioni di lettura per i contenuti dei clienti nei AWS servizi comunemente utilizzati come archivi dati, come Amazon S3, Amazon RDS, DynamoDB, Amazon Redshift e, non sono concesse da questo ruolo. ElastiCac he
Utilizzato da (entità): AMS Operations e AMS Services	
ams_ssm_automation_role	Si presume che esegua i documenti di SSM Automation all' AWS Systems Manager interno del tuo account.
ams_ssm_automation_role	
Usato da (entità): AMS Security	

Role name (Nome ruolo)	Descrizione
ams-access-security-analyst	Questo ruolo di sicurezza AMS dispone delle autorizzazioni nel tuo account AMS per eseguire il monitoraggio dedicato degli avvisi di sicurezza e la gestione degli incidenti di sicurezza. Solo pochissime persone seleziona te di AMS Security possono assumere questo ruolo. Le autorizzazioni di lettura per i contenuti dei clienti in AWS servizi comunemente utilizzat i come archivi dati, come Amazon S3, Amazon RDS, Amazon DynamoDB, Amazon Redshift e, non sono concesse da questo ruolo. ElastiCac he
ams-access-security-analyst-sola lettura	Questo ruolo di sicurezza AMS è limitato alle autorizzazioni di sola lettura nel tuo account AMS per eseguire il monitoraggio dedicato degli avvisi di sicurezza e la gestione degli incidenti di sicurezza. Le autorizzazioni di lettura per i contenuti dei clienti in AWS servizi comunemente utilizzati come archivi dati, come Amazon S3, Amazon RDS, Amazon DynamoDB, Amazon Redshift e, non sono concesse da questo ruolo. ElastiCache
Usato da (entità): Servizi AWS	
ams-access-admin	Questo ruolo di amministratore di AMS dispone delle autorizzazioni complete per operare negli account senza restrizioni. Solo i servizi interni AMS (con una politica di sessione ristretta) possono assumere il ruolo di amministratore.

Role name (Nome ruolo)	Descrizione
ams-opscenter-eventbridge-role	Creato da Amazon AWS Systems Manager OpsItems come parte EventBridge di un flusso di lavoro di Regole di AWS Config riparazione specifico per AMS.
AMSOSConfigurationCustomerInstanceRole	Questo ruolo IAM viene applicato alle EC2 istanze Amazon quando il servizio di configura zione del sistema operativo AMS rileva che mancano le policy IAM richieste. Consente alle EC2 istanze Amazon di interagire con AWS Systems Manager Amazon e CloudWatc h i EventBridge servizi Amazon. Ha inoltre allegato la policy gestita su misura da AMS per consentire l'accesso RDP alle istanze Windows.
mc-patch-glue-service-ruolo	Supposto da AWS Glue ETL Workflow per eseguire la trasformazione dei dati e prepararli per il generatore di report AMS Patch.
Utilizzato da (entità): AMS Service	
ams-alarm-manager- AWSManaged ServicesA larmManagerDe - <8-digit hash>	Presupposto dall'infrastruttura AMS Alarm Manager all'interno del tuo account AMS per eseguire la Regole di AWS Config valutazio ne di una nuova AWS AppConfig implement azione.
ams-alarm-manager- AWSManaged ServicesA larmManagerRe - <8-digit hash>	Presupposto dall'infrastruttura di bonifica di AMS Alarm Manager all'interno del tuo account AMS per consentire la creazione o l'elimina zione di allarmi per la riparazione.
ams-alarm-manager- SS- AWSManaged ServicesAlarmManager <8-digit hash>	Si presume che richiami il servizio di riparazio ne degli allarmi AMS all'interno del tuo account AMS. AWS Systems Manager

Role name (Nome ruolo)	Descrizione
ams-alarm-manager- - AWSManaged ServicesAlarmManagerTr <8-digit hash>	Presupposto dall'infrastruttura di gestione degli allarmi AMS all'interno AWS del tuo account per condurre una Regole di AWS Config valutazione AMS periodica.
ams-alarm-manager- - AWSManaged ServicesAlarmManagerVa <8-digit hash>	Assunto dall'infrastruttura di gestione degli allarmi AMS all'interno del tuo account AMS per garantire che gli allarmi richiesti esistano nell' AWS account.
ams-backup-iam-role	Questo ruolo viene utilizzato per funzionare all' AWS Backup interno dei tuoi account.
ams-monitoring- - AWSManaged ServicesL ogGroupLimitLamb <8-digit hash>	Presupposto dall'infrastruttura AMS Logging & Monitoring nel tuo account AMS per valutare il limite CloudWatch dei gruppi Amazon Logs e confrontarli con le quote di servizio.
ams-monitoring- Servizi RDSE- AWSManaged RDSMonitoring <8-digit hash>	Presupposto dall'infrastruttura AMS Logging & Monitoring nel tuo account AMS per inoltrare gli eventi Amazon RDS ad Amazon CloudWatch Events.
ams-monitoring- - AWSManaged ServicesR edshiftMonitorin <8-digit hash>	Presupposto dall'infrastruttura AMS Logging & Monitoring nel tuo account AMS per inoltrare gli eventi Amazon Redshift CreateCluster (DeleteCustere) ad Amazon CloudWatch Events.
ams-monitoring-infrastruc- - AWSManaged ServicesMonito <8-digit hash>	Presupposto dall'infrastruttura AMS Logging & Monitoring del tuo account AMS per pubblicar e messaggi su Amazon Simple Notification Service per confermare che l'account riporti tutti i dati necessari.

Role name (Nome ruolo)	Descrizione
ams-opscenter-role	Presupposto dal sistema AMS Notification Management del tuo account AMS per la gestione degli avvisi AWS Systems Manager OpsItems relativi al tuo account.
ams-opsitem-autoexecution-role	Presupposto dal sistema di gestione delle notifiche AMS per gestire la riparazione automatica utilizzando documenti SSM per il monitoraggio degli avvisi relativi alle risorse dell'account.
ams-patch-infrastructure-amspatchconfigrulero leC1- <8-digit hash>	Si presume che valuti AWS Config le risorse delle patch AMS e rilevi eventuali variazioni nei relativi CloudFormation stack.
ams-patch-infrastructure-amspatchcwruleopsite mams- <8-digit hash>	Creato da Amazon EventBridge per risolvere AWS Systems Manager OpsItems gli errori di patching.
ams-patch-infrastructure-amspatchser vicebusamspat- <8-digit hash>	Ipotizzato da Amazon EventBridge per inviare un evento al bus di eventi di AMS Patch Orchestrator per le notifiche di modifica dello stato di Windows di AWS Systems Manager manutenzione.
ams-patch-reporting-infra-amspatchreportingco nfigr- <8-digit hash>	Si presume che valuti AWS Config le risorse di reporting di AMS Patch e rilevi eventuali variazioni nei suoi stack. CloudFormation
ams-resource-tagger- - AWSManaged ServicesResourceTagg <8-digit hash>	Presupposto dall'infrastruttura AMS Resource Tagger all'interno del tuo account AMS per eseguire la Regole di AWS Config valutazione in caso di nuova AWS AppConfig implement azione.

Role name (Nome ruolo)	Descrizione
ams-resource-tagger- - AWSManaged ServicesResourceTagg <8-digit hash>	Presupposto dall'infrastruttura AMS Resource Tagger all'interno del tuo account AMS per convalidare l'esistenza dei AWS tag richiesti per le risorse gestite.
ams-resource-tagger- - AWSManaged ServicesResourceTagg <8-digit hash>	Si presume che AWS Systems Manager richiami il flusso di lavoro di riparazione di AMS Resource Tagger nel tuo account AMS.
ams-resource-tagger- - AWSManaged ServicesResourceTagg <8-digit hash>	Supposto dall'infrastruttura di riparazione AMS Resource Tagger all'interno del tuo account AMS per creare o eliminare i AWS tag per le risorse gestite.
ams-resource-tagger- - AWSManaged ServicesResourceTagg <8-digit hash>	Presupposto dall'infrastruttura AMS Resource Tagger all'interno del tuo AWS account per condurre una valutazione periodica delle regole AMS Config.
ams_os_configuration_event_rule_role- <AWS Region>	Amazon presume che EventBridge inoltri gli eventi dal tuo account al servizio di configura zione del sistema operativo AMS EventBus nella regione corretta.
mc-patch-reporting-service	Presupposto dall'aggregatore di dati sulle patch e dal generatore di report AMS.

Note

Questo è il modello per il ams-access-management ruolo. È lo stack che gli architetti cloud (CAs) distribuiscono manualmente nel tuo account al momento dell'onboarding: management-role.yaml.
Questo è il modello per i diversi ruoli e livelli di accesso:,,,: accelerate-roles.yaml. ams-access-read-only ams-access-operations ams-access-admin-operations ams-access-admin

Per ulteriori informazioni sugli identificatori AWS Cloud Development Kit (AWS CDK) (AWS CDK), inclusi gli hash, consulta Unique. IDs

I feature service di AMS Accelerate assumono il ams-access-adminruolo di accesso programmatico all'account, ma con una politica di sessione specifica per il rispettivo feature service (ad esempio, patch, backup, monitoraggio e così via).

AMS Accelerate segue le migliori pratiche del settore per soddisfare e mantenere l'idoneità alla conformità. L'accesso di AMS Accelerate al tuo account è registrato CloudTrail e disponibile anche per la revisione tramite il monitoraggio delle modifiche. Per informazioni sulle interrogazioni che puoi utilizzare per ottenere queste informazioni, consultaMonitoraggio delle modifiche nei tuoi account AMS Accelerate.

Gestione dell'accesso con policy

Diversi team di supporto di AMS Accelerate, come Operations Engineers, Cloud Architects e Cloud Service Delivery Managers (CSDMs), a volte richiedono l'accesso ai tuoi account per rispondere alle richieste di servizio e agli incidenti. Il loro accesso è regolato da un servizio di accesso AMS interno che applica controlli quali la giustificazione aziendale, le richieste di assistenza, gli elementi operativi e i casi di supporto. L'accesso predefinito è di sola lettura e tutti gli accessi vengono tracciati e registrati; vedi anche. Monitoraggio delle modifiche nei tuoi account AMS Accelerate

Convalida delle risorse IAM

Il sistema di accesso AMS Accelerate assume periodicamente ruoli nei tuoi account (almeno ogni 24 ore) e verifica che tutte le nostre risorse IAM siano quelle previste.

Per proteggere i vostri account, AMS Accelerate dispone di un «canarino» che monitora e segnala la presenza e lo status dei ruoli IAM, nonché le relative politiche, menzionate sopra. Periodicamente, Canary assume il ams-access-read-onlyruolo CloudFormation e avvia chiamate API IAM contro i vostri account. The Canary valuta lo stato dei ruoli di accesso di AMS Accelerate per assicurarsi che siano sempre invariati e... up-to-date Questa attività crea CloudTrail registri nell'account.

Il nome di sessione AWS Security Token Service (AWS STS) del canarino è AMS-Access-Roles-Auditor- {uuid4 ()} come mostrato in e si verificano le seguenti chiamate API: CloudTrail

- Chiamate API Cloud Formation: `describe_stacks()`
- Chiamate API IAM:
  - `get_role()`

- `list_attached_role_policies()`
- `list_role_policies()`
- `get_policy()`
- `get_policy_version()`
- `get_role_policy()`

Risposta agli incidenti di sicurezza in AMS

La sicurezza è la massima priorità di AWS Managed Services (AMS). AMS distribuisce risorse e controlli nei tuoi account per gestirli. AWS ha un modello di responsabilità AWS condivisa: gestisce la sicurezza del cloud e tu sei responsabile della sicurezza nel cloud. AMS protegge i tuoi dati e le tue risorse e aiuta a mantenere la tua AWS infrastruttura sicura utilizzando controlli di sicurezza e il monitoraggio attivo dei problemi di sicurezza. Queste funzionalità ti aiutano a stabilire una base di sicurezza per le applicazioni in esecuzione nel AWS cloud. AMS collabora con voi tramite Security Incident Response per valutare l'effetto e quindi effettuare misure di contenimento e correzione sulla base delle raccomandazioni delle migliori pratiche.

Quando si verifica una deviazione dalla linea di base, ad esempio a causa di un'errata configurazione o di un cambiamento di fattori esterni, è necessario rispondere e indagare. Per farlo con successo, è necessario comprendere i concetti di base di Security Incident Response all'interno del proprio ambiente AMS. È inoltre necessario comprendere i requisiti per preparare, istruire e formare i team cloud prima che si verifichino problemi di sicurezza. È importante conoscere i controlli e le funzionalità che è possibile utilizzare, preparare piani di risposta per problemi di sicurezza comuni, come la compromissione di un account utente o l'uso improprio di account privilegiati, e identificare metodi di riparazione che utilizzano l'automazione per migliorare la velocità e la coerenza di risposta. Inoltre, è necessario comprendere i requisiti normativi e di conformità relativi alla creazione di un programma di Security Incident Response per soddisfare tali requisiti.

Security Incident Response può essere complesso, ma implementando un approccio iterativo è possibile semplificare il processo e consentire al team di risposta agli incidenti di soddisfare le parti interessate delle risorse fornendo un rilevamento e una risposta tempestivi e continui. In questa guida, ti forniamo la metodologia utilizzata da AMS per la risposta agli incidenti, la matrice di responsabilità AMS (RACI), come prepararti per un evento di sicurezza, come coinvolgere AMS durante gli incidenti di sicurezza e alcuni dei runbook di risposta agli incidenti utilizzati da AMS.

Come funziona AMS Security Incident Response

AWS Managed Services si allinea alla Guida alla gestione degli incidenti di sicurezza informatica NIST 800-61 per la risposta agli incidenti di sicurezza. Allineandoci a questo standard di settore, forniamo un approccio coerente alla gestione degli eventi di sicurezza e aderiamo alle migliori pratiche per proteggere e rispondere agli incidenti di sicurezza nel tuo cloud.

Ciclo di vita della risposta agli incidenti

Quando il rilevamento identifica e genera un avviso di sicurezza o richiedi assistenza per la sicurezza, il team di AWS Managed Services Operations si assicura che venga condotta un'indagine tempestiva, esegue automazioni per eseguire la raccolta, il triage e l'analisi dei dati, ti informa dell'analisi, esegue indagini e qualsiasi attività di contenimento e quindi pubblica l'analisi degli eventi.

Le attività di raccolta, triage, analisi e contenimento dei dati eseguite durante la risposta all'incidente variano a seconda del tipo di evento di sicurezza oggetto di indagine. Alla fine di questo documento sono riportati esempi di flussi di lavoro di Security Incident Response per scenari selezionati.

Durante gli incidenti, AMS determina dinamicamente la linea d'azione corretta, il che potrebbe comportare il riordino o l'aggiramento appropriato delle fasi documentate per garantire che si verifichi il risultato giusto.

Preparazione

Con l'evolversi del panorama delle minacce, AMS continua a espandere le capacità di rilevamento e risposta. Man mano che vengono aggiunti nuovi rilevamenti, AMS incorpora gli avvisi di questi nuovi rilevamenti nella piattaforma di rilevamento e risposta. I soccorritori di sicurezza AMS sono formati per indagare e collaborare con voi durante tutto il ciclo di vita del Security Incident Response.

Grazie a questo approccio basato sulla partnership, è importante che i team addetti alla sicurezza e alle applicazioni siano preparati a collaborare con AMS per gestire gli eventi di sicurezza man mano che si verificano tali eventi. Questa documentazione spiega cosa aspettarsi durante un evento di sicurezza e aiuta a prepararsi per una risposta rapida quando si verifica un incidente di sicurezza.

Questa documentazione utilizza la definizione NIST 800-61 di evento come qualsiasi evento osservabile in un sistema o in una rete e un incidente come violazione o minaccia imminente di violazione delle politiche, delle politiche di utilizzo accettabile o delle pratiche di sicurezza standard.

Lista di controllo per la preparazione

Completa la seguente lista di controllo con il tuo AMS cloud solution delivery manager (CSDM) e l'architetto cloud AMS (CA):

- Scopri quali carichi di lavoro vengono eseguiti in quali account.
- Scopri quali team interni sono responsabili dei vari carichi di lavoro e etichettali in modo appropriato nei carichi di lavoro.
- Gestisci internamente i dati di contatto di altri team che potrebbero essere necessari durante un'indagine su un evento di sicurezza e per le decisioni di contenimento.
- Verifica che i contatti di sicurezza siano aggiornati e aggiunti a tutti gli account gestiti AWS . I contatti vengono gestiti per account.
- Scopri come segnalare un incidente di sicurezza ad AMS e conosci la gravità e i tempi di risposta previsti.
- Assicurati che, quando le notifiche di sicurezza vengono ricevute, vengano indirizzate alle persone e ai sistemi appropriati, come i cercapersone o il centro operativo di sicurezza.
- Scopri quali fonti di registro sono disponibili, dove sono archiviate nei tuoi account e chi può accedervi.
- Scopri come utilizzare CloudWatch Insights to Query Logs durante le indagini.
- Comprendi le opzioni di contenimento disponibili per risorsa (IAMEC2, S3 e così via) e le conseguenze sulla disponibilità del carico di lavoro durante il contenimento.

Rilevamento

Durante la gestione degli AWS account, AMS monitora eventuali anomalie nel comportamento degli utenti, nelle attività degli account e nei potenziali eventi di sicurezza utilizzando i dati raccolti da fonti e controlli di rilevamento, tra cui, a titolo esemplificativo ma non esaustivo, CloudWatch Amazon, GuardDuty VPC Flow Logs, Amazon Macie AWS Config e i feed interni di Amazon Threat Intelligence.

AMS utilizza sia AWS servizi nativi che altre tecnologie di rilevamento per rispondere agli eventi di sicurezza creati da:

- Tipi di ricerca della conformità di Config
- GuardDuty Tipi di ricerca
- Tipi di ricerca di Macie

- Eventi del firewall DNS di Amazon Route 53 Resolver
- Eventi di sicurezza AMS (allarmi cloud watch)

Ulteriori risultati vengono aggiunti man mano che i servizi, i prodotti e gli ecosistemi di minacce si evolvono.

Segnala gli eventi di sicurezza ad AMS

Segnala un incidente tramite l'AMS Support Portal o Supporto Center per notificare ad AMS un incidente di sicurezza o per richiedere indagini.

Analizzare

Dopo aver identificato e segnalato un evento di sicurezza, il passaggio successivo consiste nell'analizzare se l'evento segnalato è un falso positivo o un incidente reale. AMS utilizza l'automazione e le tecniche investigative manuali per gestire gli eventi di sicurezza. L'analisi include l'analisi dei log provenienti da diverse fonti di rilevamento, come i registri del traffico di rete, i registri degli host, CloudTrail gli eventi, i registri dei AWS servizi e così via. L'analisi cerca anche modelli che mostrano un comportamento anomalo per correlazione.

La collaborazione è necessaria per comprendere il contesto specifico dell'ambiente dell'account e stabilire ciò che è normale per l'account e i carichi di lavoro. Ciò consente ad AMS di identificare un'anomalia più rapidamente e di accelerare la risposta agli incidenti.

Gestisci le comunicazioni di AMS relative agli eventi di sicurezza

AMS ti tiene informato durante le indagini contattando i tuoi contatti di sicurezza tramite una segnalazione in caso di incidente. Il vostro AMS cloud service delivery manager (CSDM) e l'architetto cloud AMS (CA) sono i punti di contatto a cui rivolgervi per qualsiasi comunicazione durante un'indagine di sicurezza attiva.

La comunicazione include la notifica automatica quando viene generato un avviso di sicurezza, l'analisi della comunicazione dopo l'evento, la creazione di call bridge e la consegna continua di elementi quali file di registro, istantanee delle risorse infette e la trasmissione dei risultati delle indagini all'utente durante l'evento di sicurezza.

I campi standard inclusi nelle notifiche di avviso di sicurezza AMS sono elencati di seguito. Questi campi forniscono informazioni che consentono di indirizzare gli eventi ai team appropriati all'interno dell'organizzazione per la correzione.

- Tipo di ricerca
- Identificatore del ritrovamento (se pertinente)
- Individuazione della gravità
- Descrizione del ritrovamento
- Individuazione della data e dell'ora di creazione
- AWS ID dell'account
- Regione (se pertinente)
- AWS Risorse (IAM user/role/policy EC2, S3, EKS)

Vengono forniti campi aggiuntivi a seconda del tipo di risultato, ad esempio EKS Findings include i dettagli di Pod, Container e Cluster.

Contenere

L'approccio di AMS al contenimento si basa sulla collaborazione con te. Conosci la tua attività e gli impatti sul carico di lavoro che potrebbero derivare dalle attività di contenimento, come l'isolamento della rete, il de-provisioning di utenti o ruoli IAM, la ricostruzione delle istanze e così via.

Una parte essenziale del contenimento è il processo decisionale. Ad esempio, spegnere un sistema, isolare una risorsa dalla rete o disattivare l'accesso o terminare le sessioni. Queste decisioni sono più facili da prendere se esistono strategie e procedure predeterminate per contenere l'incidente. AMS fornisce la strategia di contenimento e quindi implementa la soluzione dopo aver considerato il rischio associato all'implementazione delle azioni di contenimento.

Esistono diverse opzioni di contenimento a seconda delle risorse oggetto di analisi. AMS prevede che durante un'indagine su un incidente vengano implementati contemporaneamente più tipi di contenimento. Alcuni di questi esempi includono:

- Applica regole di protezione per bloccare il traffico non autorizzato (gruppo di sicurezza, NACL, regole WAF, regole SCP, Deny listing, impostazione dell'azione di firma in quarantena o blocco)
- Isolamento delle risorse
- Isolamento di rete
- Disabilitazione degli utenti, dei ruoli e delle politiche IAM
- Modifica/riduzione dei privilegi di utente e ruolo IAM

- Interruzione, sospensione, eliminazione delle risorse di calcolo
- Limitazione dell'accesso pubblico alla risorsa interessata
- Chiavi di accesso, chiavi API e password a rotazione
- Eliminazione delle credenziali divulgate e delle informazioni sensibili

AMS vi incoraggia a prendere in considerazione il tipo di strategie di contenimento per ogni tipo di incidente grave che rientra nella vostra propensione al rischio, con criteri chiaramente documentati per facilitare il processo decisionale in caso di incidente. I criteri per determinare la strategia appropriata includono:

- Potenziali danni alle risorse
- Conservazione delle prove
- Indisponibilità del servizio (ad esempio, connettività di rete, servizi forniti a parti esterne)
- Tempo e risorse necessari per implementare la strategia
- Efficacia della strategia (ad esempio, contenimento parziale, contenimento totale)
- Permanenza della soluzione (ad esempio, decisioni relative a porte unidirezionali o porte bidirezionali)
- Durata della soluzione (ad esempio, soluzione alternativa di emergenza da rimuovere in quattro ore, soluzione temporanea da rimuovere in due settimane, soluzione permanente).
- Applica controlli di sicurezza attivabili per ridurre il rischio e concedi il tempo necessario per definire e implementare un contenimento più efficace.

La velocità di contenimento è fondamentale, AMS consiglia un approccio graduale per ottenere un contenimento efficiente ed efficace attraverso strategie a breve e lungo termine.

Utilizzate questa guida per prendere in considerazione la vostra strategia di contenimento che prevede diverse tecniche in base al tipo di risorsa.

- Strategia di contenimento
  - AMS può identificare la portata dell'incidente di sicurezza?
    - In caso affermativo, identifica tutte le risorse (utenti, sistemi, risorse).
    - In caso negativo, esaminate parallelamente all'esecuzione del passaggio successivo sulle risorse identificate.
  - La risorsa può essere isolata?

    - In caso affermativo, procedi a isolare le risorse interessate.
    - In caso negativo, collabora con i proprietari e i gestori del sistema per determinare le ulteriori azioni necessarie per contenere il problema.
  - Tutte le risorse interessate sono isolate dalle risorse non interessate?
    - In caso affermativo, procedi con il passaggio successivo.
    - In caso negativo, continuate a isolare le risorse interessate fino a raggiungere un contenimento a breve termine per evitare che l'incidente si aggravi ulteriormente.
- Backup del sistema
  - Sono state create copie di backup dei sistemi interessati per ulteriori analisi?
  - Le copie forensi sono crittografate e archiviate in un luogo sicuro?
    - In caso affermativo, procedi con il passaggio successivo.
    - In caso negativo, crittografa le immagini forensi, quindi conservale in un luogo sicuro per evitare utilizzi accidentali, danni e manomissioni.

Sradicare

Dopo aver contenuto un incidente, potrebbe essere necessario eliminarlo per eliminare del tutto le fonti di minaccia e proteggere il sistema prima di procedere alla fase di ripristino successiva. Le misure di eradicazione potrebbero includere l'eliminazione del malware e la rimozione degli account utente compromessi, nonché l'identificazione e la mitigazione di tutte le vulnerabilità sfruttate. Durante l'eliminazione, è importante identificare tutti gli account, le risorse e le istanze interessati all'interno dell'ambiente in modo che possano essere corretti.

È buona norma che l'eradicazione e il ripristino avvengano secondo un approccio graduale, in modo da dare priorità alle fasi di riparazione. Per gli incidenti su larga scala, il ripristino potrebbe richiedere mesi. L'intento delle fasi iniziali deve essere quello di aumentare la sicurezza complessiva con modifiche di valore relativamente rapide (da giorni a settimane) per prevenire incidenti futuri. Le fasi successive devono concentrarsi sui cambiamenti a lungo termine (ad esempio, modifiche all'infrastruttura) e sul lavoro continuo per mantenere l'azienda il più sicura possibile.

Per alcuni incidenti, l'eradicazione non è necessaria o viene eseguita durante il recupero.

Considera i seguenti aspetti:

- È possibile modificare l'immagine del sistema e quindi rafforzarlo con patch o altre contromisure per prevenire o ridurre il rischio di attacchi?

- Tutti i malware e gli altri artefatti lasciati dagli aggressori sono stati rimossi e i sistemi interessati sono protetti da ulteriori attacchi?

Ripristino

AMS collabora con te per ripristinare il normale funzionamento dei sistemi, confermare che funzionino normalmente e (se applicabile) correggere le vulnerabilità per prevenire incidenti simili.

Considera i seguenti aspetti:

- I sistemi interessati sono aggiornati e rafforzati contro l'attacco recente e i possibili attacchi futuri?
- In che giorno e a che ora è possibile ripristinare la produzione dei sistemi interessati?
- Quali strumenti utilizzerete per testare, monitorare e verificare che i sistemi ripristinati in produzione non siano vulnerabili alle tecniche di attacco iniziali?

Segnalazione post incidente

Dopo l'evento, AMS esegue un processo di revisione delle indagini per tutti gli incidenti di sicurezza. Inoltre, AMS avvia un processo di correzione dell'errore (COE) per risolvere gli incidenti di sicurezza causati da un errore di sistema o procedurale che plausibilmente ha margini di miglioramento. AMS collabora con te per migliorare continuamente l'esperienza delle indagini sulla sicurezza. Il processo COE aiuta AMS a identificare i fattori che contribuiscono agli eventi che influiscono sui clienti e collega tali cause alle azioni successive, elementi che possono impedire il ripetersi di eventi simili o contribuire a mitigare la durata o il livello di impatto.

Il processo di revisione delle indagini sugli incidenti di sicurezza affronta i seguenti elementi per identificare le opportunità di miglioramento:

- Qual è stato il tempo trascorso dall'inizio dell'incidente alla scoperta dell'incidente, alla valutazione iniziale dell'impatto e a ciascuna fase del processo di gestione dell'incidente (ad esempio, contenimento, ripristino)?
- Quanto tempo ha impiegato il team di risposta all'incidente per rispondere alla segnalazione iniziale dell'incidente?
- Quanto tempo è stato necessario per eseguire un'analisi d'impatto iniziale?
- Era evitabile e in che modo? Esiste uno strumento o un processo che avrebbe potuto impedirlo?
- Avremmo potuto rilevarlo prima e in che modo?

- Cosa avrebbe potuto velocizzare le indagini?
- Sono state seguite le procedure documentate di risposta agli incidenti? Erano adeguate?
- La condivisione delle informazioni con altre parti interessate è stata effettuata in modo tempestivo? Come potrebbe essere migliorata?
- La collaborazione con altri team (addetti AWS alla sicurezza, agli account, al team di AWS sviluppo e al team di sicurezza dei clienti) è stata efficace? In caso contrario, cosa potrebbe essere migliorato?
- Quali fasi preparatorie mancavano che avrebbero potuto essere utili, le matrici di escalation, i RACI, i modelli di responsabilità condivisa e così via? È necessario aggiornare qualche Runbook?
- Qual era la differenza tra la valutazione d'impatto iniziale e la valutazione d'impatto finale? Cosa possiamo fare per migliorare l'accuratezza delle valutazioni nelle fasi iniziali della risposta all'incidente?
- Quali sono gli elementi d'azione tratti dalle lezioni apprese?

Runbook di risposta agli incidenti di sicurezza in AMS

Questa sezione contiene due runbook:

- Risposta all'attività dell'utente root
- Risposta agli eventi di malware

Risposta all'attività dell'utente root

L'utente root è il superutente del tuo AWS account. Tieni presente che AMS monitora l'utilizzo dei root. È consigliabile utilizzare l'utente root solo per le poche attività che lo richiedono, ad esempio modificare le impostazioni dell'account, attivare l'accesso AWS Identity and Access Management (IAM) alla fatturazione e alla gestione dei costi, modificare la password root e attivare l'autenticazione a più fattori (MFA). Per ulteriori informazioni, consulta Attività che richiedono credenziali utente root.

Per ulteriori informazioni su come informare AMS dell'utilizzo root pianificato, consulta Quando e come utilizzare l'account root in AMS.

Quando viene rilevata un'attività dell'utente root, sia che si tratti di tentativi falliti di accesso, che potrebbero indicare un attacco di forza bruta, sia di attività nell'account dopo un accesso riuscito, viene generato un evento e viene inviato un incidente ai contatti di sicurezza definiti.

AWS Managed Services Operations analizza le attività non pianificate degli utenti root, esegue la raccolta, il triage e l'analisi dei dati ed esegue attività di contenimento secondo le tue indicazioni, seguite dall'analisi post-evento.

Se utilizzi il modello operativo AMS Advanced, ricevi comunicazioni aggiuntive dagli ingegneri di AMS CSDM e AMS Ops che confermano l'attività non pianificata dell'utente root, dovuta alla responsabilità di AMS di proteggere le credenziali degli utenti root. AMS analizza l'attività dell'utente root fino a quando non viene confermato un percorso da seguire.

Preparazione

Informate AMS di qualsiasi utilizzo pianificato dell'utente root inviando una richiesta di servizio AMS con i dati e gli orari dell'evento pianificato per evitare attività di risposta agli incidenti non necessarie.

Rivolgiti periodicamente GameDays ad AMS per verificare che i processi di risposta agli incidenti dei clienti di AMS siano aggiornati, le persone e i sistemi e costruisci una memoria muscolare con le persone responsabili per ottenere una risposta più rapida agli incidenti.

Fase A: rilevamento

AMS monitora l'attività principale negli account attraverso fonti di rilevamento, tra cui GuardDuty il monitoraggio AMS.

Se disponi di AMS Accelerate, il modello operativo risponde all'incidente richiedendo un'indagine per eventuali attività impreviste dell'utente root. Quando ciò si verifica, AMS Operations avvia il Compromised Account runbook.

Se disponi di AMS Advanced, il modello operativo risponde all'incidente o informa il CSDM di qualsiasi attività pianificata dell'utente root per chiudere un'indagine attiva sulla compromissione dell'account.

Fase B: analisi

AMS esegue un'indagine approfondita sugli eventi degli utenti root quando determina che l'attività non è autorizzata. Utilizzando sia le automazioni che il team di risposta alla sicurezza AMS, i log e gli eventi vengono analizzati alla ricerca di anomalie e comportamenti imprevisti per gli utenti root. I log vengono forniti per aiutare a determinare se l'attività è sconosciuta, se si tratta di un evento utente root autorizzato o se richiede ulteriori indagini.

Alcuni esempi delle informazioni fornite durante l'indagine a supporto dei controlli interni includono:

- Informazioni sull'account: su quale account è stato utilizzato l'account root?
- Indirizzo e-mail per l'utente root: ogni utente root è associato a un indirizzo e-mail dell'organizzazione
- Dettagli di autenticazione: da dove e quando l'utente root ha avuto accesso al vostro ambiente?
- Record di attività: cosa ha fatto l'utente dopo aver effettuato l'accesso come root? Questi record sono sotto forma di CloudWatch eventi. Capire come leggere questi registri aiuta nelle indagini.

È consigliabile essere pronti a ricevere le informazioni di analisi e disporre di un piano per contattare i punti di contatto autorizzati per gli account all'interno dell'organizzazione. Poiché gli utenti root non vengono nominati come individui, determinare chi ha accesso all'indirizzo di posta elettronica principale utilizzato per l'account all'interno dell'organizzazione aiuta a indirizzare rapidamente le domande all'interno dell'organizzazione.

Fase C: contenimento ed eliminazione

AMS collabora con i tuoi team di sicurezza per eseguire il contenimento seguendo le indicazioni dei tuoi contatti autorizzati per la Customer Security. Le opzioni di contenimento includono:

- Rotazione delle credenziali e delle chiavi appropriate.
- Interruzione delle sessioni attive su account e risorse.
- Eliminazione delle risorse create.

Durante le attività di contenimento, AMS collabora a stretto contatto con il vostro team di sicurezza per garantire che eventuali interruzioni dei carichi di lavoro siano ridotte al minimo e che le credenziali root siano protette in modo adeguato.

Una volta completato il piano di contenimento, collaborerai con il team operativo di AMS per tutte le azioni di ripristino necessarie.

Rapporto successivo all'incidente

Se necessario, AMS avvia il processo di revisione delle indagini per identificare le lezioni apprese. Come parte del completamento di un COE, AMS comunica tutti i risultati pertinenti ai clienti interessati per aiutarli a migliorare il processo di risposta agli incidenti.

AMS documenta tutti i dettagli finali dell'indagine, raccoglie le metriche appropriate e quindi segnala l'incidente a tutti i team interni di AMS che richiedono informazioni, compresi il CSDM e la CA assegnati.

Risposta agli eventi di malware

Le EC2 istanze Amazon vengono utilizzate per ospitare una varietà di carichi di lavoro, tra cui software di terze parti e software sviluppato su misura distribuito dai team applicativi all'interno delle organizzazioni. AMS fornisce e ti incoraggia a distribuire i tuoi carichi di lavoro su immagini che vengono patchate e gestite su base continuativa da AMS.

Durante il funzionamento delle istanze, AMS monitora le anomalie nel comportamento o nell'attività attraverso una serie di controlli di rilevamento della sicurezza, tra cui Amazon GuardDuty, Network Traffic e i feed interni di Amazon Threat Intelligence.

AMS monitora anche Malware GuardDuty Findings. Questi sono disponibili sia su AMS Advanced che su AMS Accelerate, se abilitati. Per ulteriori informazioni, consulta GuardDuty la sezione Protezione da malware in Amazon.

> **Note**
>
> Se hai optato per Bring Your Own EPS, la procedura di risposta agli incidenti è diversa da quella descritta in questa pagina. Per ulteriori informazioni, consulta la documentazione di riferimento.

Quando viene rilevato un malware, viene creato un incidente e l'utente riceve una notifica dell'evento. Questa notifica è seguita da tutte le attività di riparazione che si sono verificate. AMS Operations indaga, esegue la raccolta, il triage e l'analisi dei dati, quindi esegue attività di contenimento secondo le indicazioni del cliente, seguite dall'analisi post-evento.

Fase A: Rilevamento

AMS monitora gli eventi sulle istanze con. GuardDuty AMS determina le attività di arricchimento e valutazione appropriate per aiutarvi a prendere decisioni di contenimento o di accettazione del rischio in base al tipo di scoperta o di avviso.

La raccolta dei dati viene eseguita in base al tipo di risultato. La raccolta dei dati prevede l'interrogazione di più fonti di dati sia all'interno che all'esterno dell'account interessato per creare un quadro dell'attività osservata o delle configurazioni che destano preoccupazione.

AMS esegue la correlazione dei risultati con altri allarmi e avvisi o telemetria provenienti da qualsiasi account interessato o piattaforma AMS di intelligence sulle minacce.

Fase B: analisi

Una volta raccolti, i dati vengono analizzati per identificare eventuali attività o indicatori di preoccupazione. Durante questa fase dell'indagine, AMS collabora con voi per integrare le conoscenze aziendali e di settore relative alle istanze e ai carichi di lavoro, al fine di aiutarvi a capire cosa ci si aspetta da ciò che è fuori dall'ordinario.

Alcuni esempi delle informazioni fornite durante l'indagine a supporto dei controlli interni includono:

- Informazioni sull'account: su quale account è stata osservata l'attività del malware?
- Dettagli sull'istanza: Quali istanze sono implicate negli eventi relativi al malware?
- Timestamp dell'evento: quando è scattato l'avviso?
- Informazioni sul carico di lavoro: cosa è in esecuzione sull'istanza?
- Dettagli sul malware, se pertinenti: famiglie di malware e informazioni open source sul malware.
- Dettagli sugli utenti o sui ruoli: quali utenti o ruoli sono interessati e coinvolti nell'attività?
- Record delle attività: quali attività vengono registrate sull'istanza? Questi sono sotto forma di CloudWatch eventi ed eventi di sistema generati dall'istanza. Capire come leggere questi registri ti aiuterà nelle indagini
- Attività di rete: quali endpoint si connettono all'istanza, a cosa si connette l'istanza e cos'è l'analisi del traffico?

È consigliabile essere pronti a ricevere informazioni sulle indagini e predisporre un piano su come contattare i punti di contatto appropriati per account, istanze e carichi di lavoro all'interno dell'organizzazione. Comprendere la topologia di rete e la connessione prevista può aiutare ad accelerare l'analisi dell'impatto. Anche la conoscenza dei test di penetrazione pianificati nell'ambiente e delle recenti implementazioni eseguite dai proprietari delle applicazioni può accelerare le indagini.

Se si determina che l'attività è pianificata e autorizzata, l'incidente viene aggiornato e l'indagine termina. Se il compromesso viene confermato, tu e AMS stabilite il piano di contenimento appropriato.

Fase C: Contenere ed eliminare

AMS collabora con te per determinare le attività di contenimento appropriate sulla base dei dati raccolti e delle informazioni note. Le opzioni di contenimento includono, a titolo esemplificativo ma non esaustivo:

- Conservazione dei dati tramite istantanee

- Modifica delle regole di rete per limitare il traffico in entrata o in uscita dalle istanze
- Modifica delle policy relative agli utenti e ai ruoli di SCP, IAM per limitare l'accesso
- Chiusura, sospensione o disattivazione delle istanze
- Interruzione di qualsiasi connessione persistente
- Rotazione delle credenziali/chiavi appropriate

Se scegli di eseguire l'attività di eradicazione sull'istanza, AMS ti aiuta a raggiungere tale obiettivo. Le opzioni includono, a titolo esemplificativo ma non esaustivo:

- Rimozione di qualsiasi software indesiderato
- Ricostruzione dell'istanza da un'immagine pulita e completamente patchata e ridistribuzione delle applicazioni e della configurazione
- Ripristino dell'istanza da un backup precedente
- Distribuzione di applicazioni e servizi su un'altra istanza all'interno dell'account che potrebbe essere adatta a ospitare i carichi di lavoro.

È importante determinare in che modo il malware è stato distribuito ed eseguito sull'istanza prima del ripristino del servizio per assicurarsi che vengano applicati eventuali controlli aggiuntivi per prevenire la ricomparsa del malware sull'istanza. AMS fornisce approfondimenti o informazioni aggiuntivi ai tuoi partner o team forensi, se necessario per supportare l'analisi forense.

A questo punto, collabori con AMS Operations per le attività di ripristino. AMS collabora a stretto contatto con te per ridurre al minimo le interruzioni dei carichi di lavoro e proteggere le istanze.

Rapporto successivo all'incidente

Se necessario, AMS avvia il processo di revisione delle indagini per identificare le lezioni apprese. Nell'ambito del completamento di un COE, AMS vi comunica i risultati pertinenti per aiutarvi a migliorare il processo di risposta agli incidenti.

AMS documenta i dettagli finali dell'indagine, raccoglie i parametri appropriati e segnala l'incidente ai team interni di AMS che richiedono informazioni, compresi il CSDM e la CA assegnati.

Registrazione e monitoraggio degli eventi di sicurezza in Accelerate

Gli account registrati ad AMS Accelerate sono configurati con un'implementazione di base di CloudWatch eventi e allarmi ottimizzati per ridurre il rumore e identificare le indicazioni di un incidente

reale. AMS Accelerate lo utilizza GuardDuty anche per il monitoraggio degli account. Per ulteriori informazioni, consulta Monitora con GuardDuty.

Conformità della configurazione in Acceler

AMS Accelerate ti aiuta a configurare le tue risorse secondo standard elevati di sicurezza e integrità operativa e a rispettare i seguenti standard di settore:

- Center for Internet Security (CIS)
- Framework di sicurezza cloud (CSF) del National Institute of Standards and Technology (NIST)
- Health Insurance Portability and Accountability Act (HIPAA)
- Standard di sicurezza dei dati (DSS) del settore delle carte di pagamento (PCI)

Lo facciamo implementando l'intero set di AWS Config regole di conformità sul tuo account, vedi. Libreria AMS Config Rule Una AWS Config regola rappresenta le configurazioni desiderate per una risorsa e viene valutata in base alle modifiche alla configurazione delle impostazioni delle risorse. AWS Qualsiasi modifica alla configurazione attiva un gran numero di regole per verificare la conformità. Ad esempio, supponiamo di creare un bucket Amazon S3 e di configurarlo in modo che sia leggibile pubblicamente, in violazione degli standard NIST. La bucket-public-read-prohibited regola ams-nist-cis-s 3 rileva la violazione e etichetta il bucket S3 come non conforme nel report di configurazione. Poiché questa regola appartiene alla categoria di riparazione automatica degli incidenti, crea immediatamente un rapporto sugli incidenti, che avvisa l'utente del problema. Altre violazioni più gravi delle regole potrebbero indurre AMS a risolvere automaticamente il problema. Per informazioni, consulta Risposte alle violazioni in Accelerate.

> **Important**
>
> Se desideri che facciamo di più, ad esempio, se desideri che AMS ponga rimedio a una violazione per te, indipendentemente dalla categoria di riparazione, invia una richiesta di assistenza che chieda ad AMS di porre rimedio alle risorse non conformi per te. Nella richiesta di assistenza, includi un commento come «Come parte della correzione delle regole di configurazione AMS, rimedia alle risorse non soggette a reclami*RESOURCE_ARNS_OR_IDs*, regola di configurazione *CONFIG_RULE_NAME* nell'account» e aggiungi gli input necessari per porre rimedio alla violazione.

Se vuoi che facciamo di meno, ad esempio, se non vuoi che interveniamo su un particolare bucket S3 che richiede l'accesso pubblico per progettazione, puoi creare eccezioni, vedi. Creazione di eccezioni alle regole in Accelerate

Libreria AMS Config Rule

Accelerate implementa una libreria di regole di configurazione AMS per proteggere il tuo account. Queste regole di configurazione iniziano con. `ams-` Puoi visualizzare le regole all'interno del tuo account e il relativo stato di conformità dalla AWS Config console, dalla AWS CLI o dall' AWS Config API. Per informazioni generali sull'utilizzo AWS Config, consulta ViewingConfiguration Conformità.

Note

Per le regioni opt-in Regioni AWS e gov cloud, implementiamo solo un sottoinsieme delle regole di configurazione a causa delle restrizioni regionali. Verifica la disponibilità delle regole nelle regioni controllando il link associato all'identificatore nella tabella delle regole di configurazione di AMS Accelerate.
Non è possibile rimuovere nessuna delle regole di Config AMS distribuite.

Tabella delle regole

Scarica come ams_config_rules.zip.

Regole di configurazione AMS

Nome regola	Servizio	Trigger	Azione	Framework
ams-nist-cis-guardduty-abilitato-centralizzato	GuardDuty	Periodic (Periodico)	Risanare	CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-1; HIPAA: 164.312 (a) (2) (iv), 164.312 (e) (2) (ii); PCI: 2,2,3.4,8.2.1;
ams-nist-cis-vpc-flow-logs-enabled	VPC	Periodic (Periodico)	Risolvere	CIS: CIS.6; NIST-CSF: DE.AE-1, DE.AE-3, PR.DS-5, PR.PT-1; HIPAA: 164.308 (a) (3)

Nome regola	Servizio	Trigger	Azione	Framework
				(ii) (A), 164.312 (b); PCI: 2.2,10.1,10.3.2,10.3.3,10.3.3,10.3.4,10.3.5,10.3.6;
ams-eks-secrets-encrypted	EKS	Periodic (Periodico)	Incidente	CIS: NA; NIST-CSF: NA; HIPAA: NA; PCI: NA;
ams-eks-endpoint-no-accesso pubblico	EKS	Periodic (Periodico)	Incidente	CIS: NA; NIST-CSF: NA; HIPAA: NA; PCI: NA;
ams-nist-cis-vpc-default-security-group-closed	VPC	Modifiche alla configurazione	Incidente	CIS: CIS.11, CIS.12, CIS.9; NIST-CSF: DE.AE-1, PR.AC-3, PR.AC-5, PR.PT-4; HIPAA: 164.312 (e) (1); PCI: 1,2, 1,3, 2,1, 2,2, 2.1,1.3.1,1.3.2,2.2.2;
ams-nist-cis-iam-politica in materia di password	IAM	Periodic (Periodico)	Incidente	CIS: NA; NIST-CSF: PR.AC-1, PR.AC-4; HIPAA: 164,308 (a) (3) (i), 164.308 (a) (3) (ii) (A) ,164,308 (a) (3) (ii) (B) ,164308 (a) (4) (i), 164.308 (a) (4) (ii) (A), 164.308 (a), 164.308 (a) (a), 164.308 (a) (a), 164.308 (a) (a), 164.308 (a) (A), 164.308 (a) 308 (a) (4) (ii) (B), 164.308 (a) (4) (ii) (C), 164,312 (a) (1); PCI: 7.1.2,7.1.3, 7.2.1,7.2.2;

Nome regola	Servizio	Trigger	Azione	Framework
ams-nist-cis-iam-root-access-key-check	IAM	Periodic (Periodico)	Incidente	CIS: CIS.16, CIS.4; NIST-CSF: PR.AC-1, PR.AC-4, PR.PT-3; HIPAA: 164,308 (a) (3) (i), 164.308 (a) (a) (3) (ii) (A), 164.308 (a) (3) (ii) (B), 164.308 (a) (4) (i), 164.308 (a), 164.308 (a), 164.308 (a), 164.308 (a), 164.308 (a), 164.308 (a) (4) (ii) (A), 164.308 (a) (4) (ii) (B), 164.308 (a) (4) (ii) (C), 164,312 (a) (1); PCI: 2,2,7.1.2,7.1.3,7.2.1,7.2.2;
ams-nist-cis-iam-user-mfa-enabled	IAM	Periodic (Periodico)	Incidente	CIS: CIS.16; NIST-CSF: PR.AC-1, PR.AC-4; HIPAA: 164,308 (a) (3) (i), 164.308 (a) (3) (ii) (A) ,164.308 (a) (3) (ii) (B), 164.308 (a) (4) (i), 164.308 (a) (4) (ii) (A) ,164,308 (a) (4) (ii) (B), 164.308 (a) (4) (ii) (C), 164,312 (a) (1); PCI: 2,2,7.1.2,7.1.3,7.2.1,7.2.2;
ams-nist-cis-restricted-ssh	Gruppi di sicurezza	Modifiche alla configurazione	Incidente	CIS: CIS.16; NIST-CSF: PR.AC-1, PR.AC-4; HIPAA: 164,308 (a) (3) (i), 164.308 (a) (4) (ii) (A), 164.308 (a) (4) (ii) (B), 164.308 (a) (4) (ii) (C), 164,312 (a) (1); PP CI: 2.2, 7.2.1, 8.1.4;

Nome regola	Servizio	Trigger	Azione	Framework
ams-nist-cis-restricted-porte comuni	Gruppi di sicurezza	Modifiche alla configurazione	Incidente	CIS: CIS.11, CIS.12, CIS.9; NIST-CSF: DE.AE-1, PR.AC-3, PR.AC-5, PR.PT-4; HIPAA: 164.308 (a) (3) (i), 164.308 (a) (3) (ii) (B), 164.308 (a) (i), 164.308 (a) (4) (a) (4) ii) (A), 164.308 (a) (4) (ii) (B), 164.308 (a) (4) (ii) (C) ,164,312 (a) (1) ,164.312 (e) (1); PCI: 1,2, 3,2,2, 2,1, 2,1, 3,1, 3,1, 3,1, 3,2, 3,2, 2,2.2;
ams-nist-cis-s3 account-level-public-access - blocchi	S3	Modifiche alla configurazione	Incidente	CIS: CIS.9, CIS.12, CIS.14; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.DS-5, PR.PT-3, PR.PT-4; HIPAA: 164.308 (a) (3) (i), 164.308 (a) (i) (4) (ii) (A), 164.308 (a) (4) (ii) C), 164,312 (a) (1) ,164,312 (e) (1); PCI: 1,2, 2,1, 1,3, 3,1, 3,1, 3,2, 3,4, 3,6, 2,2,2,2,2;

Nome regola	Servizio	Trigger	Azione	Framework
ams-nist-cis-s3- bucket-public-read-prohibited	S3	Modifiche alla configurazione	Incidente	CIS: CIS.12, CIS.14, CIS.9; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.DS-5, PR.PT-3, PR.PT-4; HIPAA: 164.308 (a) (3) (i), 164.308 (a) (i) (4) (ii) (A), 164.308 (a) (4) (ii) C), 164,312 (a) (1), 164,312 (e) (1); PCI: 1,2, 3,2,2, 2,1, 2,1, 3,1, 3,1, 2,1, 3,6, 2,2.2;
ams-nist-cis-s3- bucket-public-write-prohibited	S3	Modifiche alla configurazione	Incidente	CIS: CIS.12, CIS.14, CIS.9; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.DS-5, PR.PT-3, PR.PT-4; HIPAA: 164.308 (a) (3) (i), 164.308 (a) (i) (4) (ii) (A), 164.308 (a) (4) (ii) C), 164,312 (a) (1), 164,312 (e) (1); PCI: 1,2, 3,2,2, 2,1, 2,1, 3,1, 3,1, 2,1, 3,6, 2,2.2;
ams-nist-cis-s3- bucket-server-side-encryption abilitato	S3	Modifiche alla configurazione	Incidente	CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-1; HIPAA: 164.312 (a) (2) (iv), 164.312 (c) (2), 164.312 (e) (2) (ii); PCI: 2,2,34,10.5,8.2.1;

Nome regola	Servizio	Trigger	Azione	Framework
ams-nist-cis-securityhub-abilitato	Security Hub	Periodic (Periodico)	Incidente	CIS: CIS.3, CIS.4, CIS.6, CIS.12, CIS.16, CIS.19; NIST-CSF: PR.DS-5, PR.PT-1; HIPAA: 164.312b; PCI: NA;
ams-nist-cis-ecinstance-managed-by-systems2- -manager	EC2	Modifiche alla configurazione	Report	CIS: CIS.2, CIS.5; NIST-CSF: ID.AM-2, PR.IP-1; HIPAA: 164,308 (a) (5) (ii) (B); PCI: 2.4;
ams-nist-cis-cloudtrail-abilitato	CloudTrail	Periodic (Periodico)	Report	CIS: CIS.16, CIS.6; NIST-CSF: DE.AE-1, DE.AE-3, PR.DS-5, PR.MA-2, PR.PT-1; HIPAA: 164.308 (a) (3) (ii) (A), 164.308 (a) (5) (ii) (C), 164.312 (b); PCI: 10.1,10.2.1,10.10. 10.10 2,2,10.2.3,10.2,4, 10.2,5,10.2.6,10.2.7,10.3,1 0.3,2,10.3.3,10.3.4,10,3,5, 10.3.6;
ams-nist-cis-access-tasti ruotati	IAM	Periodic (Periodico)	Report	CIS: CIS.16; NIST-CSF: PR.AC-1; HIPAA: 164,308 (a) (4) (ii) (B); PCI: 2.2;
ams-nist-cis-acm-certificate-expiration-check	Certificate Manager	Modifiche alla configurazione	Report	CIS: CIS.13, CIS.14; NIST-CSF: PR.AC-5, PR.PT-4; HIPAA: NA; PCI: 4.1;

Nome regola	Servizio	Trigger	Azione	Framework
ams-nist-cis-alb- -controlla http-to-https-redirection	ALB	Periodic (Periodico)	Report	CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-2; HIPAA: 164.312 (a) (2) (iv), 164.312 (e) (1), 164.312 (e) (2) (i), 164.312 (e) (2) (ii); PCI: 2,3, 4.1, 8.2.1;
ams-nist-cis-api- - crittografato gw-cache-enabled-and	API Gateway	Modifiche alla configurazione	Report	CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-1; HIPAA: 164,312 (a) (2) (iv), 164.312 (e) (2) (ii); PCI: 3.4;
ams-nist-cis-api-gw-execution-logging-enabled	API Gateway	Modifiche alla configurazione	Report	CIS: CIS.6; NIST-CSF: DE.AE-1, DE.AE-3, PR.PT-1; HIPAA: 164.312 (b); PCI: 10.1,10.3 .1,10.3.2,10.3.3,10.3.4,10. 3.5,10.3.6,10.5.4;
ams-nist-autoscaling-group-elb-healthcheck-required	ELB	Modifiche alla configurazione	Report	CIS: NA; NIST-CSF: PR.PT-1, PR.PT-5; HIPAA: 164,312 (b); PCI: 2.2;
ams-nist-cis-cloud-trail-encryption-enabled	CloudTrail	Periodic (Periodico)	Report	CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-1; HIPAA: 164,312 (a) (2) (iv), 164,312 (e) (2) (ii); PCI: 2,2,3.4, 10,5;

Nome regola	Servizio	Trigger	Azione	Framework
ams-nist-cis-cloud- -abilitato trail-log-file-validation	CloudTrail	Periodic (Periodico)	Report	CIS: CIS.6; NIST-CSF: PR.DS-6; HIPAA: 164.312 (c) (1), 164.312 (c) (2); PCI: 2.2, 10.5,11.5, 10.5.2, 10.5.5;
ams-nist-cis-cloudtrail-s3-dataevents-abilitato	CloudTrail	Periodic (Periodico)	Report	CIS: CIS.6; NIST-CSF: DE.AE-1, DE.AE-3, PR.DS-5, PR.PT-1; HIPAA: 164.308 (a) (3) (ii) (A) ,164.312 (b); PCI: 2.2,10.1.10.2.1,10.2.2,10.2.2,10.2.3,10.2.5,10.3.10.3.3,3,10.3.3 0,3,4,10, 3,5,10,3,6;
ams-nist-cis-cloudwatch-alarm-action-check	CloudWatch	Modifiche alla configurazione	Report	CIS: CIS.13, CIS.14; NIST-CSF: NA; HIPAA: 164.312 (a) (2) (iv), 164.312 (e) (2) (ii); PCI: 3.4;
ams-nist-cis-cloudwatch-log-group-encrypted	CloudWatch	Periodic (Periodico)	Report	CIS: CIS.13, CIS.14; NIST-CSF: NA; HIPAA: 164,312 (a) (2) (iv), 164,312 (e) (2) (ii); PCI: 3.4;
ams-nist-cis-codebuild-project-envvar-awscred-check	CodeBuild	Modifiche alla configurazione	Report	CIS: CIS.18; NIST-CSF: PR.DS-5; HIPAA: 164.308 (a) (3) (i), 164.308 (a) (4) (ii) (A) ,164.308 (a) (4) (ii) (C), 164.312 (a) (1); PCI: 8.2.1;

Nome regola	Servizio	Trigger	Azione	Framework
ams-nist-cis-codebuild- -controlla project-source-repo-url	CodeBuild	Modifiche alla configurazione	Report	CIS: CIS.18; NIST-CSF: PR.DS-5; HIPAA: 164.308 (a) (3) (i), 164.308 (a) (4) (ii) (A) ,164.308 (a) (4) (ii) (C), 164.312 (a) (1); PCI: 8.2.1;
ams-nist-cis-db-instance-backup-enabled	RDS	Modifiche alla configurazione	Report	CIS: CIS.10; NIST-CSF: ID.BE-5, PR.DS-4, PR.IP-4, PR.PT-5, RC.RP-1; HIPAA: 164,308 (a) (7) (i), 164.308 (a) (7) (a) (7) (a) (7) (b); PCI: NA;
ams-nist-cis-dms-replication-not-public	DMS	Periodic (Periodico)	Report	CIS: CIS.12, CIS.14, CIS.9; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.DS-5, PR.PT-3, PR.PT-4; HIPAA: 164.308 (a) (3) (i), 164.308 (a) (i) (4) (ii) (A), 164.308 (a) (4) (ii) C), 164,312 (a) (1), 164,312 (e) (1); PCI: 1,2,1,3,1 .2.1,1.3.2,1.3.3,4,1.3.6,2. 2.2;
ams-nist-dynamodb-autoscaling-abilitato	DynamoDB	Periodic (Periodico)	Report	CIS: NA; NIST-CSF: ID.BE-5, PR.DS-4, PR.PT-5, RC.RP-1; HIPAA: 164,308 (a) (7) (i), 164.308 (a) (7) (7) (7) (ii) (C); PCI: NA;

Nome regola	Servizio	Trigger	Azione	Framework
ams-nist-cis-dynamodb-abilitato a pitr	DynamoDB	Periodic (Periodico)	Report	CIS: CIS.10; NIST-CSF: ID.BE-5, PR.DS-4, PR.IP-4, PR.PT-5, RC.RP-1; HIPAA: 164.308 (a) (7) (i), 164.308 (a) (7) (a) (7) (a) (7) (i); PCI: NA;
ams-nist-dynamodb-throughput-limite-controllo	DynamoDB	Periodic (Periodico)	Report	CIS: NA; NIST-CSF: NA; HIPAA: 164.312b; PCI: NA;
ams-nist-ebs-optimized-istanza	EBS	Modifiche alla configurazione	Report	CIS: NA; NIST-CSF: NA; HIPAA: 164.308 (a) (7) (i); PCI: NA;
ams-nist-cis-ebs-snapshot-public-restorable-check	EBS	Periodic (Periodico)	Report	CIS: CIS.12, CIS.14, CIS.9; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.DS-5, PR.PT-3, PR.PT-4; HIPAA: 164.308 (a) (3) (i), 164.308 (a) (i) (4) (ii) (A), 164.308 (a) (4) (ii) C), 164,312 (a) (1), 164,312 (e) (1); PCI: 1,2,1,3,1 .2.1,1.3.2,1.3.3,4,1.3.6,2. 2.2;
ams-nist-ec2- instance-detailed-monitoring-enabled	EC2	Modifiche alla configurazione	Report	CIS: NA; NIST-CSF: DE.AE-1, PR.PT-1; HIPAA: 164.312 (b); PCI: NA;

Nome regola	Servizio	Trigger	Azione	Framework
ams-nist-cis-ec2- instance-no-public-ip	EC2	Modifiche alla configurazione	Report	CIS: CIS.12, CIS.14, CIS.9; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.PT-3, PR.PT-4; HIPAA: 164.308 (a) (3) (i) ,164,312 (a) (1), 164,312 (e) (1); PCI: 1,2, 1,3, 2,1, 1,1, 3,2, 3,4, 3,6, 2,2.2;
ams-nist-cis-ec2-managedinstance-association-compliance-status -controlla	EC2	Modifiche alla configurazione	Report	CIS: CIS.12, CIS.9; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.PT-3, PR.PT-4; HIPAA: 164.308 (a) (3) (i), 164.308 (a) (4) (ii) (A), 164.308 (a) (4) (ii) (C), 164.312 (a) (a) (a) 1), 164,312 (e) (1); PCI: 1,2, 1,3, 2,1, 3,1, 3,2, 3,4, 3,6, 2,2.2;
ams-nist-cis-ec2-managedinstance-patch-compliance-status -controlla	EC2	Modifiche alla configurazione	Report	CIS: CIS.2, CIS.5; NIST-CSF: ID.AM-2, PR.IP-1; HIPAA: 164,308 (a) (5) (ii) (B); PCI: 6.2;
ams-nist-cis-ecistanza a 2 interruzioni	EC2	Periodic (Periodico)	Report	CIS: CIS.2; NIST-CSF: ID.AM-2, PR.IP-1; HIPAA: NA; PCI: NA;

Nome regola	Servizio	Trigger	Azione	Framework
ams-nist-cis-ec2- volume-in use-check	EC2	Modifiche alla configurazione	Report	CIS: CIS.2; NIST-CSF: PR.IP-1; HIPAA: NA; PCI: NA;
ams-nist-cis-efs-controllo crittografato	EFS	Periodic (Periodico)	Report	CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-1; HIPAA: 164.312 (a) (2) (iv), 164.312 (e) (2) (ii); PCI: 3.4,8.2.1;
ams-nist-cis-eip-allegato	EC2	Modifiche alla configurazione	Report	CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-1; HIPAA: 164.312 (a) (2) (iv), 164.312 (e) (2) (ii); PCI: 3.4.8.2.1;
ams-nist-cis-elasticache- -controlla redis-cluster-auto matic-backup	ElastiCache	Periodic (Periodico)	Report	CIS: CIS.10; NIST-CSF: ID.BE-5, PR.DS-4, PR.IP-4, PR.PT-5, RC.RP-1; HIPAA: 164.308 (a) (7) (i), 164.308 (a) (7) (a) (7) (a) (7) (i), PCI: NA;
ams-nist-cis-opensearch-encrypted-at-rest	OpenSearch	Periodic (Periodico)	Report	CIS: CIS.14, CIS.13; NIST-CSF: PR.DS-1; HIPAA: 164.312 (a) (2) (iv), 164.312 (e) (2) (ii); PCI: 3.4.8.2.1;
ams-nist-cis-opensearch-in-vpc-only	OpenSearch	Periodic (Periodico)	Report	CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-1; HIPAA: 164.312 (a) (2) (iv), 164.312 (e) (2) (ii); PCI: 3.4.8.2.1;

Nome regola	Servizio	Trigger	Azione	Framework
ams-nist-cis-elb-acm-certificate-required	Certificate Manager	Modifiche alla configurazione	Report	CIS: CIS.12, CIS.9; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.DS-5, PR.PT-3, PR.PT-4; HIPAA: 164.308 (a) (3) (i), 164.308 (a) (4) (ii) (A), 164.308 (a) (4) (ii) (C), 164.308 (a) (C) 312 (a) (1), 164,312 (e) (1); PCI: 1,2, 1,3, 1,2, 1,1, 3,1, 3,2, 3,4, 3,6, 2,2.2;
ams-nist-elb-deletion-abilitato alla protezione	ELB	Modifiche alla configurazione	Report	CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-2; HIPAA: 164.312 (a) (2) (iv), 164.312 (e) (1), 164.312 (e) (2) (i), 164.312 (e) (2) (ii); PCI: 4.1.8.2.1;
ams-nist-cis-elb- abilitato alla registrazione	ELB	Modifiche alla configurazione	Report	CIS: CIS.6; NIST-CSF: DE.AE-1, DE.AE-3, PR.PT-1; HIPAA: 164.312 (b); PCI: 10.1,10.3 .1,10.3.2,10.3.3,10.3.4,10. 3.5,10.3.6,10.5.4;
ams-nist-cis-emr-abilitato per Kerberos	EMR	Periodic (Periodico)	Report	CIS: CIS.6; NIST-CSF: DE.AE-1, DE.AE-3, PR.PT-1; HIPAA: 164.312 (b); PCI: 10.1,10.3 .1,10.3.2,10.3.3,10.3.4,10. 3.5,10.3.6,10.5.4;

Nome regola	Servizio	Trigger	Azione	Framework
ams-nist-cis-emr-master-no-public-ip	EMR	Periodic (Periodico)	Report	CIS: CIS.14, CIS.16; NIST-CSF: PR.AC-1, PR.AC-4, PR.AC-6; HIPAA: 164,308 (a) (3) (i), 164.308 (a) (a) (3) (ii) (A), 164.308 (a) (3) (ii) (B), 164.308 (a) (4) (i), 164.308 (a), 164.308 (a), 164.308 (a), 164.308 (a), 164.308 (a), 164.308 (a) (4) (ii) (A), 164.308 (a) (4) (ii) (B), 164.308 (a) (4) (ii) (C), 164.312 (a) (1); PCI: 7.2.1;
ams-nist-cis-encrypted-volumi	EBS	Modifiche alla configurazione	Report	CIS: CIS.12, CIS.9; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.PT-3, PR.PT-4; HIPAA: 164.308 (a) (3) (i), 164.308 (a) (4) (ii) (A), 164.308 (a) (4) (ii) (C), 164.312 (a) (a) (a) 1), 164,312 (e) (1); PCI: 1,2, 1,3, 2,1, 3,1, 3,2, 3,4, 3,6, 2,2.2;

Nome regola	Servizio	Trigger	Azione	Framework
ams-nist-cis-guardduty-non-archived-findings	GuardDuty	Periodic (Periodico)	Report	CIS: CIS.12, CIS.13, CIS.16, CIS.19, CIS.3, CIS.4, CIS.6, CIS.8; NIST-CSF: DE.AE-2, DE.AE-3, DE.CM-4, DE.DP-5, ID.RA-1, ID.RA-3, PR.DS-5, PR.PT-1; HIPAA: 164.308 (a) (5) (ii) (C), 164.308 (a) (6) (ii), 164.312 (b); PCI: 6.1,11.4, 5.1.2;
ams-nist-iam-group-has-users-check	IAM	Modifiche alla configurazione	Report	CIS: NA; NIST-CSF: PR.AC-4, PR.AC-1; HIPAA: 164,308 (a) (3) (i), 164.308 (a) (3) (ii) (A) ,164,308 (a) (3) (ii) (B) ,164308 (a) (4) (i), 164.308 (a) (4) (ii) (A), 164.308 (a) (A), 164.308 (a), 164.308 (a) (a), 164.308 (a) (A), 164.308 (a) 308 (a) (4) (ii) (B), 164.308 (a) (4) (ii) (C), 164,312 (a) (1); PCI: 7.1.2,7.1.3, 7.2.1,7.2.2;
ams-nist-cis-iam- policy-no-statements-with -accesso amministrativo	IAM	Modifiche alla configurazione	Report	CIS: CIS.16; NIST-CSF: PR.AC-6, PR.AC-7; HIPAA: 164,308 (a) (4) (ii) (B), 164.308 (a) (5) (ii) (D), 164.312 (d); PCI: 8.2.3, 8.2.4,8.2.5;

Nome regola	Servizio	Trigger	Azione	Framework
ams-nist-cis-iam-user-group-membership-check	IAM	Modifiche alla configurazione	Report	CIS: CIS.16, CIS.4; NIST-CSF: PR.AC-1, PR.AC-4, PR.PT-3; HIPAA: 164,308 (a) (3) (i), 164.308 (a) (4) (ii) (A) ,164,308 (a) (4) (ii) (B), 164.308 (a) (4) (ii) (C), 164.308 (a) (4) (c), 164.308 (a) (a) (4) (c), 164.308 (a) 12 (a) (1), 164,312 (a) (2) (i); PCI: 2,2,7.1.2,7.2.1,8.1.1;
ams-nist-cis-iam-user-no-policies-check	IAM	Modifiche alla configurazione	Report	CIS: CIS.16; NIST-CSF: PR.AC-1, PR.AC-7; HIPAA: 164,308 (a) (4) (ii) (B), 164.312 (d); PCI: 8.3;
ams-nist-cis-iam-user-unused-credentials-check	IAM	Periodic (Periodico)	Report	CIS: CIS.16; NIST-CSF: PR.AC-1, PR.AC-4, PR.PT-3; HIPAA: 164,308 (a) (3) (i), 164.308 (a) (3) (ii) (A), 164.308 (a) (3) (ii) (B) ,164308 (a) (4) (i), 164.308 (a) (4) (a) (4) ii) (A), 164.308 (a) (4) (ii) (B), 164.308 (a) (4) (ii) (C), 164,312 (a) (1); PCI: 2,2,7.1.2,7.1.3,7.2.1,7.2.2;

Nome regola	Servizio	Trigger	Azione	Framework
ams-nist-cis-ec2- instances -in-vpc	EC2	Modifiche alla configurazione	Report	CIS: CIS.11, CIS.12, CIS.9; NIST-CSF: DE.AE-1, PR.AC-3, PR.AC-5, PR.PT-4; HIPAA: 164.308 (a) (3) (i), 164.308 (a) (3) (ii) (B), 164.308 (a) (i), 164.308 (a) (4) (a) (4) ii) (A), 164.308 (a) (4) (ii) (B), 164.308 (a) (4) (ii) (C) ,164,312 (a) (1) ,164.312 (e) (1); PCI: 1,2, 3,2,2, 2,1, 2,1, 3,1, 3,1, 3,1, 3,2, 3,2, 2,2.2;
ams-nist-cis-internet-gateway-authorized-vpc-only	Internet Gateway	Periodic (Periodico)	Report	CIS: CIS.9, CIS.12; NIST-CSF: NA; HIPAA: NA; PCI: NA;
ams-nist-cis-kms- -cancellazione cmk-not-scheduled-for	KMS	Periodic (Periodico)	Report	CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-1; HIPAA: NA; PCI: 3,5, 3,6;
ams-nist-lambda-concurrency-controlla	Lambda	Modifiche alla configurazione	Report	CIS: NA; NIST-CSF: NA; HIPAA: 164.312b; PCI: NA;
ams-nist-lambda-dlq-controlla	Lambda	Modifiche alla configurazione	Report	CIS: NA; NIST-CSF: NA; HIPAA: 164.312b; PCI: NA;

Nome regola	Servizio	Trigger	Azione	Framework
ams-nist-cis-lambda-function-public-access-prohibited	Lambda	Modifiche alla configurazione	Report	CIS: CIS.12, CIS.9; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.DS-5, PR.PT-3, PR.PT-4; HIPAA: 164.308 (a) (3) (i), 164.308 (a) (4) (ii) (A), 164.308 (a) (4) (ii) (C), 164.308 (a) (C) 312 (a) (1), 164,312 (e) (1); PCI: 1,2, 1,3, 1,2, 1,1, 3,1, 3,2, 3,4, 2,2.2;
ams-nist-cis-lambda-interno in vpc	Lambda	Modifiche alla configurazione	Report	CIS: CIS.12, CIS.9; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.PT-3, PR.PT-4; HIPAA: 164.308 (a) (3) (i), 164.308 (a) (4) (ii) (A), 164.308 (a) (4) (ii) (C), 164.312 (a) (a) (a) 1), 164,312 (e) (1); PCI: 1,2, 1,3, 2,1, 3,1, 3,2, 3,4, 2,2,2;
ams-nist-cis-mfa- enabled-for-iam-console-accesso	IAM	Periodic (Periodico)	Report	CIS: CIS.16; NIST-CSF: PR.AC-7; HIPAA: 164.312 (d); PCI: 2.2,8.3;

Nome regola	Servizio	Trigger	Azione	Framework
ams-nist-cis-multi-region-cloudtrail-enabled	CloudTrail	Periodic (Periodico)	Report	CIS: CIS.6; NIST-CSF: DE.AE-1, DE.AE-3, PR.DS-5, PR.MA-2, PR.PT-1; HIPAA: 164.308 (a) (3) (ii) (A) ,164.312 (b); PCI: 2.2,10.1.0.2.1,10. 2.2,10.2.2,10.2.2,10.2.3,10 .2.3,10.2.3,10.2.2,10.2.3,1 0.2.3,10.2.4,10.2.2.2,10.2. 3,10.2.3,10.2.3,10.2.4,10.2 .2.3,10.2.2,10.2.3,10.2.3,1 0.2.3,10.2.3,10.2.4,10.2.2, 10.2.2,10.2.3,10.2.3,10.2.4 ,10.2.2.6,10,2,7,10,3,10,3, 2,10,3,3,10,3,4,10,0,3,5,10 ,0,3,6;
ams-nist-rds-enhanced-abilitato al monitoraggio	RDS	Modifiche alla configurazione	Report	CIS: NA; NIST-CSF: PR.PT-1; HIPAA: 164.312b; PCI: NA;
ams-nist-cis-rds-instance-public-access-check	RDS	Modifiche alla configurazione	Report	CIS: CIS.12, CIS.14, CIS.9; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.DS-5, PR.PT-3, PR.PT-4; HIPAA: 164.308 (a) (3) (i), 164.308 (a) (i) (4) (ii) (A), 164.308 (a) (4) (ii) C), 164,312 (a) (1), 164,312 (e) (1); PCI: 1,2,1,3,1 .2.1,1.3.2,1.3.3,4,1.3.6,2. 2.2;

Nome regola	Servizio	Trigger	Azione	Framework
ams-nist-rds-multi-az-supporto	RDS	Modifiche alla configurazione	Report	CIS: NA; NIST-CSF: ID.BE-5, PR.DS-4, PR.PT-5, RC.RP-1; HIPAA: 164,308 (a) (7) (i), 164.308 (a) (7) (a) (7) (7) (ii) (C); PCI: NA;
ams-nist-cis-rds-snapshots-public-prohibited	RDS	Modifiche alla configurazione	Report	CIS: CIS.12, CIS.14, CIS.9; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.DS-5, PR.PT-3, PR.PT-4; HIPAA: 164.308 (a) (3) (i), 164.308 (a) (i) (4) (ii) (A), 164.308 (a) (4) (ii) C), 164,312 (a) (1), 164,312 (e) (1); PCI: 1,2,1,3,1 .2.1,1.3.2,1.3.3,4,1.3.6,2. 2.2;
ams-nist-cis-rds-archiviazione crittografata	RDS	Modifiche alla configurazione	Report	CIS: CIS.13, CIS.5, CIS.6; NIST-CSF: DE.AE-1, DE.AE-3, PR.DS-1, PR.PT-1; HIPAA: 164.312 (a) (2) (iv), 164.312 (b), 164.312 (e) (2) (ii); PCI: 3.4,10.1.10.2.1,10.2,2 10,2,3,10.2,4,10.2,5,10.3.1 ,10.3,2,10.3.3,10.3,4,10.3, 5,10.3,68.2,1;

Nome regola	Servizio	Trigger	Azione	Framework
ams-nist-cis-redshift-cluster-configuration-check	RedShift	Modifiche alla configurazione	Report	CIS: CIS.6, CIS.13, CIS.5; NIST-CSF: DE.AE-1, DE.AE-3, PR.DS-1, PR.PT-1; HIPAA: 164.312 (a) (2) (iv), 164.312 (b), 164.312 (e) (2) (ii); PCI: 3.4,8.2.1,10.1,10.2.1,10.2.1,10.2.1 2,2,10,2,3,10.2,4,10.2,5,10.3,10.3,2,10.3.3,10.3,4,10.3,5,10.3.6;
ams-nist-cis-redshift-cluster-public-access-check	RedShift	Modifiche alla configurazione	Report	CIS: CIS.12, CIS.14, CIS.9; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.DS-5, PR.PT-3, PR.PT-4; HIPAA: 164.308 (a) (3) (i), 164.308 (a) (i) (4) (ii) (A), 164.308 (a) (4) (ii) C), 164,312 (a) (1), 164,312 (e) (1); PCI: 1,2,1,3,1.2.1,1.3.2,1.3.3,4,1.3.6,2.2.2;
ams-nist-cis-redshift-require-tls-ssl	RedShift	Periodic (Periodico)	Report	CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-2; HIPAA: 164.312 (a) (2) (iv), 164.312 (e) (1), 164.312 (e) (2) (i), 164.312 (e) (2) (ii); PCI: 2.3.4.1;
ams-nist-cis-root-account-hardware-mfa-enabled	IAM	Periodic (Periodico)	Report	CIS: CIS.16, CIS.4; NIST-CSF: PR.AC-7; HIPAA: 164,312 (d); PCI: 2,2,8,3;

Nome regola	Servizio	Trigger	Azione	Framework
ams-nist-cis-root-account-mfa-enabled	IAM	Periodic (Periodico)	Report	CIS : CIS.16, CIS.4; NIST-CSF: PR.AC-7; HIPAA: 164.312 (d); PCI: 2.2,8.3;
ams-nist-cis-s3- bucket-default-lock-enabled	S3	Modifiche alla configurazione	Report	CIS: CIS.14, CIS.13; NIST-CSF: ID.BE-5, PR.PT-5, RC.RP-1; HIPAA: NA; PCI: NA;
ams-nist-cis-s3- bucket-logging-enabled	S3	Modifiche alla configurazione	Report	CIS: CIS.6; NIST-CSF: DE.AE-1, DE.AE-3, PR.DS-5, PR.PT-1; HIPAA: 164,308 (a) (3) (ii) (A) ,164.312 (b); PCI: 2,2,10.1,10.2.2,10.2.2,10.2.3,10.2.3,10.2.4,10.2.5,10.2.3,10.2.4,10.2.5,10.2.3,10.2.4,10.2.5 0,3,2,10, 3,3,10,3,4,10,3,5,10,3,6;
ams-nist-cis-s3- bucket-replication-enabled	S3	Modifiche alla configurazione	Report	CIS: CIS.10; NIST-CSF: ID.BE-5, PR.DS-4, PR.IP-4, PR.PT-5, RC.RP-1; HIPAA: 164,308 (a) (7) (i), 164.308 (a) (7) (a) (7) (7) (a) (7) (b); PCI: 2.2, 10.5.3;

Nome regola	Servizio	Trigger	Azione	Framework
ams-nist-cis-s3- bucket-ssl-requests-only	S3	Modifiche alla configurazione	Report	CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-2; HIPAA: 164.312 (a) (2) (iv), 164.312 (c) (2) ,164.312 (e) (1) ,164.312 (e) (2) (i), 164.312 (e) (2) (ii); PCI: 2.2,4.1.8.2.1;
ams-nist-cis-s3- bucket-versioning-enabled	S3	Periodic (Periodico)	Report	CIS: CIS.10; NIST-CSF: ID.BE-5, PR.DS-4, PR.DS-6, PR.IP-4, PR.PT-5, RC.RP-1; HIPAA: 164.308 (a) (7) (i), 164.308 (a) (7) (a) (7) (7) (a) (7) (a), 164.312 (c) (1), 164.312 (c) (2); PCI: 10.5.3;
ams-nist-cis-sagemaker-endpoint-configuration-kms-key - configurato	SageMaker	Periodic (Periodico)	Report	CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-1; HIPAA: 164.312 (a) (2) (iv), 164.312 (e) (2) (ii); PCI: 3.4.8.2.1;
ams-nist-cis-sagemaker--configurato notebook-instance-kms-key	SageMaker	Periodic (Periodico)	Report	CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-1; HIPAA: 164.312 (a) (2) (iv), 164.312 (e) (2) (ii); PCI: 3.4.8.2.1;

Nome regola	Servizio	Trigger	Azione	Framework
ams-nist-cis-sagemaker- -accesso notebook-no-direct-internet	SageMaker	Periodic (Periodico)	Report	CIS: CIS.12, CIS.9; NIST-CSF: PR.AC-3, PR.AC-4, PR.AC-5, PR.DS-5, PR.PT-3, PR.PT-4; HIPAA: 164.308 (a) (3) (i), 164.308 (a) (4) (ii) (A), 164.308 (a) (4) (ii) (C), 164.308 (a) (C) 312 (a) (1), 164,312 (e) (1); PCI: 1,2, 1,3, 1,2, 1,1, 3,1, 3,2, 3,4, 3,6, 2,2.2;
ams-nist-cis-secretsmanager-rotation-enabled-check	Secrets Manager	Modifiche alla configurazione	Report	CIS: CIS.16; NIST-CSF: PR.AC-1; HIPAA: 164,308 (a) (4) (ii) (B); PCI: NA;
ams-nist-cis-secretsmanager-scheduled-rotation-success-check	Secrets Manager	Modifiche alla configurazione	Report	CIS: CIS.16; NIST-CSF: PR.AC-1; HIPAA: 164,308 (a) (4) (ii) (B); PCI: NA;
ams-nist-cis-sns-kms crittografati	SNS	Modifiche alla configurazione	Report	CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-1; HIPAA: 164,312 (a) (2) (iv), 164.312 (e) (2) (ii); PCI: 8.2.1;

Nome regola	Servizio	Trigger	Azione	Framework
ams-nist-cis-vpc- -porte autorizzate sg-open-only-to	VPC	Modifiche alla configurazione	Report	CIS: CIS.11, CIS.12, CIS.9; NIST-CSF: DE.AE-1, PR.AC-3, PR.AC-5, PR.PT-4; HIPAA: 164.312e) (1); PCI: 1,2, 1,3, 2.1,1.3.1 ,1.3.1,1.3.2,2.2.2;
ams-nist-vpc-vpn-2 tunnel in su	VPC	Modifiche alla configurazione	Report	CIS: NA; NIST-CSF: ID.BE-5, PR.DS-4, PR.PT-5, RC.RP-1; HIPAA: 164,308 (a) (7) (i); PCI: NA;
ams-cis-ec2-ebs-encryption-by-default	EC2	Periodic (Periodico)	Report	CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-1; HIPAA: 164.312 (a) (2) (iv), 164.312 (e) (2) (ii); PCI: 2,2,3.4,8.2.1;
ams-cis-rds-snapshot-crittografato	RDS	Modifiche alla configurazione	Report	CIS: CIS.13, CIS.14; NIST-CSF: PR.DS-1; HIPAA: 164.312 (a) (2) (iv), 164.312 (e) (2) (ii); PCI: 3.4.8.2.1;
ams-cis-redshift-cluster-impostazioni di manutenzione - controllo	RedShift	Modifiche alla configurazione	Report	CIS: CIS.5; NIST-CSF: PR.DS-4, PR.IP-1, PR.IP-4; HIPAA: 164,308 (a) (5) (ii) (A), 164.308 (a) (7) (ii) (A); PCI: 6.2;

Risposte alle violazioni in Accelerate

Tutte le violazioni delle regole di configurazione vengono visualizzate nel rapporto di configurazione. Questa è una risposta universale. A seconda della categoria di riparazione (gravità) della regola, AMS potrebbe intraprendere azioni aggiuntive, riassunte nella tabella seguente. Per informazioni dettagliate su come personalizzare il codice d'azione per determinate regole, consulta. Risposte personalizzate ai risultati

Azioni di riparazione

Codice d'azione	Azioni AMS
Report	1. Aggiungi al rapporto di Config
Incidente	1. Aggiungi al rapporto di Config 2. Rapporto automatico sugli incidenti in Accelerate
Rimediare	1. Aggiungi al rapporto di Config 2. Rapporto automatico sugli incidenti in Accelerate 3. Correzione automatica in Accelerate

Richiesta di assistenza aggiuntiva

> **Note**
>
> AMS può porre rimedio a qualsiasi violazione per te, indipendentemente dalla categoria di riparazione. Per richiedere assistenza, invia una richiesta di assistenza e indica a quali risorse desideri che AMS risolva con un commento del tipo «Come parte della correzione delle regole di configurazione AMS, rimediate la *RESOURCE_ARNS_OR_IDs* risorsa ARNs/IDs>, config rule *CONFIG_RULE_NAME* in the account» e aggiungi gli input necessari per porre rimedio alla violazione.

AMS Accelerate dispone di una libreria di documenti e runbook di AWS Systems Manager automazione per aiutare a correggere le risorse non conformi.

Aggiungi al rapporto di Config

AMS genera un rapporto di Config che tiene traccia dello stato di conformità di tutte le regole e le risorse del tuo account. Puoi richiedere il rapporto dal tuo CSDM. Puoi anche esaminare lo stato di conformità dalla console AWS Config AWS , dalla CLI o dall'API Config. AWS Il tuo rapporto di Config include:

- Le principali risorse non conformi presenti nel tuo ambiente, per scoprire potenziali minacce e configurazioni errate
- Conformità delle risorse e delle regole di configurazione nel tempo
- Descrizioni delle regole di configurazione, severità delle regole e procedure correttive consigliate per correggere le risorse non conformi

Quando una risorsa entra in uno stato non conforme, lo stato della risorsa (e lo stato della regola) diventa Non conforme nel rapporto di Config. Se la regola appartiene alla categoria di correzione Config Report Only, per impostazione predefinita, AMS non intraprende ulteriori azioni. Puoi sempre creare una richiesta di assistenza per richiedere ulteriore assistenza o riparazione da AMS.

Per maggiori dettagli, consulta AWS Config Reporting.

Rapporto automatico sugli incidenti in Accelerate

In caso di violazioni delle regole moderatamente gravi, AMS crea automaticamente un rapporto sugli incidenti per informarti che una risorsa è entrata in uno stato di non conformità e chiede quali azioni desideri che vengano eseguite. Hai le seguenti opzioni per rispondere a un incidente:

- Richiedi che AMS risolva le risorse non conformi elencate nell'incidente. Quindi, cercheremo di porre rimedio alla risorsa non conforme e ti avviseremo una volta risolto l'incidente sottostante.
- Puoi risolvere l'elemento non conforme manualmente nella console o tramite il tuo sistema di distribuzione automatizzato (ad esempio, aggiornamenti del modello CI/CD Pipeline); quindi, puoi risolvere l'incidente. La risorsa non conforme viene rivalutata secondo la pianificazione della regola e, se la risorsa viene valutata come non conforme, viene creato un nuovo rapporto sull'incidente.
- È possibile scegliere di non risolvere la risorsa non conforme e risolvere semplicemente l'incidente. Se aggiorni la configurazione della risorsa in un secondo momento, AWS Config attiverà una nuova valutazione e verrai nuovamente avvisato per valutare la non conformità di quella risorsa.

Correzione automatica in Accelerate

Le regole più importanti appartengono alla categoria Auto Remediate. L'inosservanza di queste regole può avere un forte impatto sulla sicurezza e sulla disponibilità degli account. Quando una risorsa viola una di queste regole:

1. AMS ti avvisa automaticamente con un rapporto sull'incidente.
2. AMS avvia una riparazione automatica utilizzando i nostri documenti SSM automatizzati.
3. AMS aggiorna il rapporto sull'incidente indicando l'esito positivo o negativo della riparazione automatica.
4. Se la riparazione automatica non è riuscita, un tecnico AMS esamina il problema.

Creazione di eccezioni alle regole in Accelerate

La funzionalità di eccezione Regole di AWS Config delle risorse consente di eliminare la segnalazione di risorse specifiche e non conformi per regole specifiche.

> **Note**
>
> Le risorse esentate vengono ancora visualizzate come Non conformi nella console di AWS Config Service. Le risorse esentate vengono visualizzate con un flag speciale nei Config Reports (Resource_Exception:TRUE). CSDMs Puoi filtrare tali risorse in base a quella colonna durante la generazione dei report.

Se disponi di risorse che sai non sono conformi, puoi eliminare una risorsa specifica per una regola di configurazione specifica nei relativi report di configurazione. Per farlo:

Invia una richiesta di servizio ad Accelerate relativa al tuo account, con un elenco delle regole e delle risorse di configurazione che desideri escludere dal rapporto. Devi fornire una giustificazione aziendale esplicita (ad esempio, non è necessario segnalarlo *`resource_name_1`* e *`resource_name_2`* non è stato eseguito il backup perché non vogliamo che venga eseguito il backup). Per assistenza nell'invio di una richiesta di assistenza Accelerate, consulta. Creazione di una richiesta di servizio in Accelerate

Incolla nella richiesta i seguenti input (per ogni risorsa aggiungi un blocco separato con tutti i campi obbligatori, come mostrato), quindi invia:

```
[
    {
        "resource_name": "resource_name_1",
        "config_rule_name": "config_rule_name_1",
        "business_justification": "REASON_TO_EXEMPT_RESOURCE",
        "resource_type": "resource_type"
    },
    {
        "resource_name": "resource_name_2",
        "config_rule_name": "config_rule_name_2",
        "business_justification": "REASON_TO_EXEMPT_RESOURCE",
        "resource_type": "resource_type"
    }
]
```

Ridurre i AWS Config costi in Accelerate

Puoi ridurre i costi di AWS Config utilizzando l'opzione per registrare periodicamente il tipo di `AWS::EC2::Instance` risorsa. La registrazione periodica acquisisce le ultime modifiche alla configurazione delle risorse una volta ogni 24 ore, riducendo il numero di modifiche apportate. Se abilitata, registra AWS Config solo la configurazione più recente di una risorsa alla fine di un periodo di 24 ore. Ciò consente di adattare i dati di configurazione a specifici casi d'uso di pianificazione operativa, conformità e audit che non richiedono un monitoraggio continuo. Questa modifica è consigliata solo se disponi di applicazioni che dipendono da architetture temporanee, il che significa che aumenti o riduci costantemente il numero di istanze.

Per attivare la registrazione periodica per il tipo di `AWS::EC2::Instance` risorsa, contattate il vostro team di consegna AMS.

Risposte personalizzate ai risultati

Puoi scegliere come desideri che AMS Accelerate risponda ad alcuni risultati (regole di Config non conformi). Puoi configurare AMS in modo che risponda ai risultati, correggendo i risultati, chiedendo la tua approvazione per la correzione o semplicemente segnalandoli nella prossima Monthly Business Review (MBR). È possibile modificare le risposte predefinite per le regole di AMS Accelerate Config. Per visualizzare le regole, vai a Configuration Compliance > Tabella delle regole o scarica la tabella delle regole come file ZIP ams_config_rules.zip.

La modifica delle risposte predefinite ti aiuta ad aumentare lo stato di sicurezza e conformità del tuo account, permettendo di correggere più risultati. Quando si correggono più risultati, si riducono i

casi in cui è necessario attendere la revisione e l'approvazione manuali. L'ampia libreria di runbook di correzione AMS corregge costantemente le risorse non conformi e l'utente viene contattato solo quando necessario.

Le risposte personalizzate vengono utilizzate solo con nuove risorse o le risorse esistenti con nuovi eventi. Ad esempio, una risorsa che è diventata non conforme dopo una modifica. Questo perché le risorse più vecchie tendono a richiedere un'ispezione più approfondita prima della riparazione ed è più facile imporre la correzione delle risorse man mano che vengono create o modificate. Per richiedere la correzione del ritrovamento di una risorsa in qualsiasi momento, inviate una richiesta di assistenza.

Richiedere una modifica delle risposte predefinite

Cloud Architects (CAs) collaborano con te durante l'onboarding per raccogliere le tue preferenze. CAsquindi configura la configurazione iniziale sui sistemi AMS interni. Dopo l'onboarding, crea una richiesta di assistenza per richiedere aggiornamenti alle configurazioni. Puoi richiedere aggiornamenti della configurazione tutte le volte che è necessario. Tieni presente che Operations aggiorna solo le configurazioni per l'account in cui è stata creata la richiesta di servizio. Se devi aggiornare più account contemporaneamente, contatta il tuo Cloud Architect. Il tuo CA ti chiederà di tagliare una richiesta di servizio specificando le tue preferenze a fini di controllo.

Modifica delle risposte predefinite per i risultati e gli account

Hai sempre bisogno di una preferenza di risposta per ogni account e risultato. AMS fornisce una risposta predefinita (vedi Configuration Compliance), quindi questa configurazione è facoltativa. È possibile modificare le risposte predefinite per ogni risultato utilizzando le seguenti opzioni:

- Correzione: AMS corregge il risultato manualmente o automaticamente. AMS esamina la correzione e ti comunica se fallisce.
- Richiedi l'approvazione: AMS crea un caso in uscita per informarti del risultato. Utilizzate questa opzione quando desiderate esaminare il risultato prima di approvarne la correzione o esentarlo. AMS esegue quindi l'azione che preferisci.
- Nessuna azione (solo report): AMS non intraprende alcuna azione per correggere o intensificare il risultato. I risultati potrebbero ancora essere visualizzati sulla console e nei report presentati durante. MBRs

> **Note**
>
> Non è possibile modificare la configurazione delle regole che devono essere corrette da AMS. Ad esempio, abilitando Amazon GuardDuty e VPC Flow Logs.

Modifica delle risposte predefinite in base alle risorse

Puoi configurare ulteriormente la risposta a risorse specifiche utilizzando i tag. Puoi utilizzare i tag o le risorse di tag preesistenti utilizzando Resource Tagger. Per i dettagli, vediAccelera Resource Tagger). La configurazione per le risorse con tag ha la precedenza sull'azione predefinita per la ricerca. Quando una risorsa ha più tag con diverse configurazioni associate, AMS non può eseguire riparazioni personalizzate. Al contrario, AMS invia all'utente una richiesta di assistenza in uscita per informarlo della situazione. Ad esempio, per la ricerca bucket-server-side-encryptionbasata su s3-puoi:

- Modificate la risposta in modo da «correggere» i bucket S3 non crittografati con la coppia di chiave-valore del tag «Regulated: True»
- Modifica la risposta in «nessuna azione» quando i bucket S3 non crittografati hanno i tag «Regulated: False» e
- Modifica la risposta predefinita dei bucket S3 non crittografati in «chiedi approvazione». Questo vale per tutti i bucket S3 che non hanno i tag «Regulated: True» o «Regulated: False»

Puoi anche aggiungere l'input necessario per eseguire una risposta di ricerca personalizzata. Ad esempio, per le riparazioni che richiedono una chiave di crittografia, puoi fornire la chiave IDs ad AMS. È possibile modificare i parametri di input dei runbook di correzione, ma AMS non supporta l'integrazione con i runbook personalizzati. Per una descrizione dei runbook di correzione AMS nel Config Report, vedere. AWS Config Rapporto di controllo della conformità

Risposta agli incidenti in Accelerate

Dopo aver ricevuto un avviso, il team AMS utilizza soluzioni automatiche e manuali per riportare le risorse a uno stato integro. Se la riparazione fallisce, AMS avvia il processo di gestione degli incidenti per collaborare con il team. È possibile modificare le linee di base aggiornando la configurazione predefinita in un file di configurazione.

Risposta agli incidenti e onboarding in AMS Accelerate

Durante l'onboarding, AMS Accelerate elimina la creazione automatica degli incidenti per le risorse non conformi esistenti; al contrario, il Cloud Service Deliver Manager (CSDM) ti fornisce un rapporto che contiene tutte le regole e le risorse di non conformità da esaminare. Dopo aver identificato le regole a cui desideri che AMS corregga, crea una richiesta di servizio nella console Center indicando tali regole e risorse. Supporto Il seguente modello di richiesta di assistenza è un esempio di richiesta del cliente ad AMS di correggere manualmente le risorse non conformi. Se AMS ha altre domande, collaboriamo con te nella richiesta di assistenza per raccogliere le informazioni richieste.

```
Hello,
Please remediate the following resources for the Config Rule "ENCRYPTED_VOLUMES".
Resource List:
    "Vol-12345678"
    "Vol-87654312"
Thank you
```

Una volta completato il processo di onboarding, AMS Accelerate crea automaticamente un incidente per ogni risorsa non conforme alle regole contrassegnate come Incidente automatico.

Resilienza nell'accelerazione

L'infrastruttura AWS globale è costruita attorno a zone Regioni AWS di disponibilità. Regioni AWS forniscono più zone di disponibilità fisicamente separate e isolate, collegate con reti a bassa latenza, ad alto throughput e altamente ridondanti. Con le zone di disponibilità, è possibile progettare e gestire applicazioni e database che eseguono automaticamente il failover tra le zone senza interruzioni. Le zone di disponibilità sono più altamente disponibili, tolleranti ai guasti e scalabili rispetto alle tradizionali infrastrutture di data center singoli o multipli.

Per ulteriori informazioni sulle zone di disponibilità Regioni AWS e sulle zone di disponibilità, consulta l'infrastruttura globale.AWS

Per informazioni sulla gestione della continuità con AMS Accelerate, vedereGestione della continuità in AMS Accelerate.

Controllo di sicurezza per sistemi end-of-support operativi

I sistemi operativi che non rientrano nel periodo di supporto generale previsto da "end-of-support" o EOS del produttore del sistema operativo e che non ricevono aggiornamenti di sicurezza presentano un rischio maggiore per la sicurezza.

AWS offre alcuni servizi per facilitare la gestione del sistema operativo. end-of-support Per informazioni su Windows end-of-support, vedere Programma di End-of-Support migrazione per Windows Server.

> **Note**
>
> Ulteriori informazioni su questo argomento sono disponibili accedendo ai report di AWS Artifact. Per ulteriori informazioni, consulta l'argomento Download dei rapporti in AWS Artifact. Per accedere ad AWS Artifact, puoi contattare il tuo CSDM per ricevere istruzioni o andare alla pagina Getting Started with AWS Artifact. Queste informazioni non sono incluse in questa guida per l'utente perché contengono contenuti di sicurezza sensibili.

Le migliori pratiche di sicurezza in Accelerate

AMS Accelerate utilizza pacchetti di conformità, che forniscono un framework di conformità generico progettato per consentire di creare controlli di governance di sicurezza, operativi o di ottimizzazione dei costi utilizzando azioni gestite o personalizzate e di correzione. Regole di AWS Config AWS Config Per informazioni su come configurare al meglio questi pacchetti di conformità, consulta AWS Config Operational Best Practices for NIST CSF e Operational Best Practices for CIS Top 20.

Revisioni di sicurezza delle richieste di modifica

Il processo di revisione delle richieste di modifica di AWS Managed Services garantisce che AMS esegua una revisione di sicurezza delle modifiche richieste man mano che vengono implementate per tuo conto nel tuo account.

Standard tecnici AMS Acceleratedefinisci i criteri di sicurezza minimi, le configurazioni e i processi per stabilire la sicurezza di base dei tuoi account. Quando AMS implementa le modifiche richieste, seguiamo questi standard.

AMS valuta tutte le richieste di modifica rispetto agli standard tecnici AMS. Qualsiasi modifica che possa ridurre il livello di sicurezza del tuo account deviando dagli standard tecnici viene sottoposta

a un processo di revisione della sicurezza. Durante questo processo, i rischi rilevanti vengono evidenziati da AMS e analizzati e approvati dal vostro responsabile dell'approvazione del rischio autorizzato per bilanciare le esigenze di sicurezza e quelle aziendali.

Processo di gestione dei rischi per la sicurezza dei clienti

Il processo AMS Accelerate Customer Security Risk Management (CSRM) aiuta a identificare e comunicare chiaramente i rischi ai proprietari giusti. Questo processo riduce al minimo i rischi di sicurezza nell'ambiente e riduce il sovraccarico operativo continuo per i rischi identificati.

Per impostazione predefinita, quando un membro dell'organizzazione richiede ad AMS di implementare una modifica all'ambiente gestito, AMS esamina la modifica per determinare se la richiesta non rientra negli standard tecnici, il che potrebbe alterare il livello di sicurezza dell'account. Se esiste un rischio di sicurezza elevato o molto elevato, il personale di sicurezza autorizzato accetta o rifiuta la revisione della modifica. Le modifiche richieste vengono inoltre valutate per rilevare eventuali effetti negativi sulla capacità di AMS di gestire l'account. Se la revisione rileva possibili impatti negativi, sono necessarie ulteriori revisioni e approvazioni all'interno di AMS.

Accettazione, validità e revisione del rischio

Le accettazioni del rischio sono valide per un anno dalla data di approvazione. Se uno scenario di rischio precedentemente accettato si ripresenta dopo un anno, l'accettazione del rischio deve essere riesaminata e riapprovata prima di poter essere applicata. Questa revisione annuale garantisce che le decisioni sui rischi rimangano in linea con gli attuali standard tecnici, i requisiti normativi e l'evoluzione del profilo di rischio dell'organizzazione.

Rinuncia

È possibile disattivare il flusso di lavoro basato sull'approvazione nel processo CSRM in caso di rischi elevati o molto elevati. Per modificare l'opzione CSRM per account specifici da CSRM standard a Solo notifica, collabora con i tuoi Cloud Service Delivery Manager per creare un'accettazione del rischio una tantum. Se scegli di procedere con l'opzione Notification Only, AMS implementa le modifiche richieste indipendentemente dalla categoria di rischio. AMS invia una notifica di rischio ai responsabili autorizzati dell'approvazione del rischio anziché richiedere l'approvazione prima dell'implementazione della modifica.

Rivolgiti ai tuoi Cloud Architect o Cloud Service Delivery Manager per ulteriori informazioni sul processo AMS CSRM, su come modificare l'opzione CSRM predefinita durante l'onboarding di nuovi account AMS o su come aggiornare gli account esistenti.

> **Note**
>
> AMS consiglia vivamente di utilizzare l'opzione predefinita di Standard CSRM in tutti gli account.

Standard tecnici AMS Accelerate

Le seguenti sono le categorie degli standard tecnici di Accelerate:

ID	Categoria
AMS-STD-X002	AWS Identity and Access Management
AMS-STD-X003	Sicurezza di rete
AMS-STD-X004	Test di penetrazione
AMS-STD-X005	Amazon GuardDuty
AMS-STD-X007	Registrazione di log

Controlli standard in AMS Accelerate

I seguenti sono i controlli standard di AMS:

AMS-STD-X002 - (IAM) AWS Identity and Access Management

ID	Standard tecnico
1.0	Durata del timeout
1.1	Una sessione di timeout predefinita per utenti federati è di un'ora e può essere aumentata fino a quattro ore.

ID	Standard tecnico
1.2	Il timeout della sessione RDP per Microsoft Windows Server è impostato su 15 minuti e può essere esteso in base al caso d'uso.
2.0	AWS Utilizzo dell'account root
2.1	Se viene utilizzato un account root per qualsiasi motivo, Amazon GuardDuty deve essere configurato per generare risultati pertinenti.
2.2	Le chiavi di accesso per l'account root non devono essere create.
3.0	Creazione e modifica degli utenti
3.1	È possibile creare IAM users/roles con accesso programmatico e con autorizzazioni di sola lettura senza alcuna politica limitata nel tempo. Tuttavia, l'autorizzazione a o consentire la lettura di oggetti (ad esempio, S3:GetObject) in tutti i bucket Amazon Simple Storage Service dell'account non è consentita.
3.1.1	Gli utenti umani IAM per l'accesso alla console e con autorizzazioni di sola lettura possono essere creati con la politica limitata nel tempo (fino a 180 giorni), mentre la removal/renewal/ extension politica limitata nel tempo comporterà la notifica del rischio. Tuttavia, l'autorizzazione a consentire la lettura di oggetti (ad esempio, S3:GetObject) in tutti i bucket S3 dell'account non è consentita.

ID	Standard tecnico
3.2	Gli utenti e i ruoli IAM per l'accesso da console e programmatico con autorizzazioni che modificano l'infrastruttura (scrittura e gestione delle autorizzazioni) nell'account del cliente non devono essere creati senza l'accettazione del rischio. Esistono eccezioni per le autorizzazioni di scrittura a livello di oggetto S3, consentite senza l'accettazione del rischio, purché i bucket specifici rientrino nell'ambito di applicazione e per le operazioni di etichettatura su tag non correlati ad AMS.
3.3	Sui server Microsoft Windows, è necessario creare solo l'account di servizio gestito (gMSA) del gruppo Microsoft.
4.0	Politiche, azioni e APIs
4.4	Una policy non deve fornire all'amministratore un'istruzione equivalente a «Effect»: «Allow» con «Action»: «*» su «Resource»: «*» senza l'accettazione del rischio.
4.6	Le chiamate API contro le politiche chiave KMS per le chiavi dell'infrastruttura AMS nelle politiche IAM del cliente non devono essere consentite.
4.8	Le azioni, quali modifiche ai record DNS dell'infr astruttura AMS in Amazon Route 53, non devono essere consentite.

ID	Standard tecnico
4.9	Gli utenti umani IAM con accesso alla console creati dopo aver seguito la procedura prevista non devono avere alcuna policy collegata direttamente, ad eccezione della policy trust, assume role e time limited policy.
4.10	È possibile creare profili di istanza Amazon EC2 con accesso in lettura a un segreto o uno spazio dei nomi specifico all' Gestione dei segreti AWS interno dello stesso account.
4.12	La politica IAM non deve includere alcuna azione che includa l'azione Allow logs: DeleteLogGroup e logs: DeleteLogStream su qualsiasi gruppo di CloudWatch log AMS Amazon.
4.13	Le autorizzazioni per creare chiavi multiregi onali non devono essere consentite.
4.14	L'accesso all'ARN del bucket S3 che non è ancora stato creato negli account dei clienti può essere fornito limitando l'accesso ai bucket agli account dei clienti specificando il numero di account utilizzando la chiave di condizione S3 specifica del servizio s3:. ResourceAccount
4.15.1	Puoi visualizzare, creare, elencare ed eliminare l'accesso alla dashboard personalizzata di S3 Storage Lens.
4.16	È possibile concedere autorizzazioni complete relative a SQL Workbench per roles/users lavorare sui database Amazon Redshift.

ID	Standard tecnico
4.17	Qualsiasi AWS CloudShell autorizzazione può essere concessa ai ruoli del cliente in alternati va alla CLI.
4.18	Un ruolo IAM con il AWS servizio come principio affidabile deve inoltre essere in linea con gli standard tecnici IAM.
4.19	I Service Linked Roles (SLRs) non sono soggetti agli standard tecnici AMS IAM, in quanto sono creati e gestiti da IAM Service Team.
4.20	La policy IAM non dovrebbe consentire la lettura di oggetti (ad esempio, S3:GetObject) in tutti i bucket S3 dell'account.
4.21	Tutte le autorizzazioni IAM per il tipo di risorsa «savingsplan» possono essere concesse ai clienti.
4.22	Il tecnico AMS non è autorizzato a copiare o spostare manualmente i dati dei clienti (file, oggetti S3, database ecc.) in nessuno dei servizi di storage dati come Amazon S3, Amazon Relational Database Service, Amazon DynamoDB e così via, o nel file system del sistema operativo.
6.0	Politiche trasversali agli account
6.1	È possibile configurare le politiche di fiducia dei ruoli IAM tra account AMS che appartengono allo stesso cliente in base ai record dei clienti.

ID	Standard tecnico
6.2	Le politiche di fiducia dei ruoli IAM tra account AMS e non AMS devono essere configura te solo se l'account non AMS è di proprietà dello stesso cliente AMS (confermando che si trovano sotto lo stesso AWS Organizations account o abbinando il dominio e-mail al nome dell'azienda del cliente).
6.3	Le politiche di fiducia dei ruoli IAM tra account AMS e account di terze parti non devono essere configurate senza l'accettazione del rischio.
6.4	È possibile configurare politiche su più account per accedere a qualsiasi account AMS gestito dal cliente CMKs tra account AMS dello stesso cliente.
6,5	È possibile configurare politiche tra account per accedere a qualsiasi chiave KMS all'interno di un account non AMS tramite un account AMS.
6.6	Le politiche relative all'accesso a qualsiasi chiave KMS all'interno di un account AMS da parte di un account di terze parti non devono essere consentite senza l'accettazione del rischio.
6.6.1	Le politiche tra account per l'accesso a qualsiasi chiave KMS all'interno di un account AMS tramite un account diverso da AMS possono essere configurate solo se l'account non AMS è di proprietà dello stesso cliente AMS.

ID	Standard tecnico
6.7	È possibile configurare policy tra più account per accedere a qualsiasi dato o risorsa del bucket S3 in cui i dati possono essere archiviat i (come Amazon RDS, Amazon DynamoDB o Amazon Redshift) tra account AMS dello stesso cliente.
6.8	È possibile configurare policy tra account per accedere a tutti i dati o le risorse del bucket S3 in cui i dati possono essere archiviati (come Amazon RDS, Amazon DynamoDB o Amazon Redshift) in un account non AMS da un account AMS con accesso in sola lettura.
6.9	Le policy tra account per accedere a tutti i dati o le risorse del bucket S3 in cui i dati possono essere archiviati (come Amazon RDS, Amazon DynamoDB o Amazon Redshift) con autorizza zioni di scrittura f da AMS a un account non AMS (o da un account non AMS a AMS) devono essere configurate solo se l'account non AMS è di proprietà dello stesso cliente AMS (confermando che si trovano sullo stesso account o abbinando dominio email con il nome dell' AWS Organizations azienda del cliente).
6,10	È possibile configurare policy tra account per accedere a tutti i dati o le risorse del bucket S3 in cui i dati possono essere archiviati (come Amazon RDS, Amazon DynamoDB o Amazon Redshift) in un account di terze parti da un account AMS con accesso in sola lettura.

ID	Standard tecnico
6.11	Le politiche tra account per accedere a qualsiasi dato o risorsa del bucket S3 in cui i dati possono essere archiviati (come Amazon RDS, Amazon DynamoDB o Amazon Redshift) in un account di terze parti da un account AMS con accesso in scrittura non devono essere configurate senza l'accettazione del rischio.
6.12	Le politiche interaccount di account di terze parti per accedere a un bucket S3 o alle risorse in cui è possibile archiviare i dati (come Amazon RDS, Amazon DynamoDB o Amazon Redshift) non devono essere configurate senza l'accettazione del rischio.
7.0	Gruppi di utenti
7.1	I gruppi IAM con autorizzazioni di sola lettura e non mutative sono consentiti.
8.0	Policy basate su risorse
8.4	Le risorse dell'infrastruttura AMS devono essere protette dalla gestione da parte di identità non autorizzate mediante l'aggiunta di politiche basate sulle risorse.
8.2	Le risorse del cliente devono essere configura te con politiche basate sulle risorse con privilegi minimi, a meno che il cliente non specifichi esplicitamente una politica diversa.

AMS-STD-X003 - Sicurezza di rete

Di seguito è riportato il controllo standard per X003 - Network Security:

ID	Standard tecnico
	Reti
1.0	Riservato per il controllo futuro
2.0	L'IP elastico sulle istanze EC2 è consentito
3.0	È necessario utilizzare il piano di controllo AMS e, per estensione, nel piano dati TLS 1.2+.
5.0	Un gruppo di sicurezza non deve avere come sorgente 0.0.0.0/0 nella regola in entrata se non è collegato a un sistema di bilanciamento del carico come previsto dalla versione 9.0
6.0	Il bucket o gli oggetti S3 non devono essere resi pubblici senza l'accettazione del rischio.
7.0	L'accesso alla gestione dei server sulle porte SSH/22 o SSH/2222 (non SFTP/2222), TELNET/23, RDP/3389, WinRM/5985-5986, VNC/ 5900-5901 TS/CITRIX/1494 o 1604, LDAP/389 o 636 e RPC/135, NETBIOS/1 37-139 non deve essere consentito dall'esterno del VPC tramite gruppi di sicurezza.
8.0	L'accesso alla gestione del database sulle porte (MySQL/3306, PostgreSQL/5432, Oracle/15 21, MSSQL/1433) o sulla porta personalizzata non deve essere consentito dal pubblico non indirizzato a VPC tramite DX, VPC-Peer o VPN tramite gruppo di sicurezza. IPs
8.1	Qualsiasi risorsa in cui è possibile archiviar e i dati dei clienti non deve essere esposta direttamente alla rete Internet pubblica.

ID	Standard tecnico
9.0	L'accesso diretto alle applicazioni tramite le porte HTTP/80, HTTPS/8443 e HTTPS/443 da Internet è consentito solo ai sistemi di bilanciamento del carico, ma non direttamente alle risorse di calcolo, ad esempio istanze EC2, contenitori, ecc. ECS/EKS/Fargate
10.0	È possibile consentire l'accesso alle applicazioni tramite le porte HTTP/80 e HTTPS/443 dall'intervallo IP privato del cliente.
11.0	Qualsiasi modifica ai gruppi di sicurezza che controllano l'accesso all'infrastruttura AMS non deve essere consentita senza l'accettazione del rischio.
12.0	AMS Security farà riferimento agli standard ogni volta che viene richiesta l'associazione di un gruppo di sicurezza a un'istanza.
14.0	L'associazione tra account di zone private ospitate VPCs da un account AMS a un altro account AMS (o da un account non AMS a AMS) deve essere configurata solo se l'account non AMS è di proprietà dello stesso cliente AMS (confermando che si trovano sullo stesso account AWS Organization o abbinando il dominio e-mail al nome dell'azienda del cliente) utilizzando strumenti interni.
15.0	È possibile consentire connessioni peering VPC tra account che appartengono allo stesso cliente.

ID	Standard tecnico
16.0	La base AMS AMIs può essere condivisa con account non AMS a condizione che entrambi gli account siano di proprietà dello stesso cliente (confermando che appartengono allo stesso AWS Organizations account o abbinando il dominio e-mail al nome dell'azienda del cliente) utilizzando strumenti interni.
17.0	La porta FTP 21 non deve essere configurata in nessuno dei gruppi di sicurezza senza un'accett azione del rischio.
18.0	La connettività di rete tra account tramite gateway di transito è consentita a condizion e che tutti gli account siano di proprietà del cliente.
19.0	Non è consentito rendere pubblica una sottorete privata
20.0	Le connessioni peering VPC con account di terze parti (non di proprietà del cliente) non devono essere consentite.
21.0	L'allegato Transit Gateway con un account di terze parti (non di proprietà del cliente) non deve essere consentito.
22.0	Qualsiasi traffico di rete necessario ad AMS per fornire i servizi ai clienti non deve essere bloccato al punto di uscita della rete del cliente.
23.0	La richiesta ICMP in entrata ad Amazon EC2 dall'infra del cliente richiederà una notifica del rischio.

ID	Standard tecnico
24,0	È consentita la richiesta in entrata provenien te da un IPs instradamento pubblico verso Amazon VPC tramite DX, VPC-Peer o VPN tramite un gruppo di sicurezza.
25.0	Le richieste in entrata provenienti da un pubblico IPs non indirizzato ad Amazon VPC tramite DX, VPC-Peer o VPN tramite un gruppo di sicurezza richiederebbero l'accettazione del rischio.
26.0	È consentita la richiesta ICMP in uscita da Amazon EC2 verso qualsiasi destinazione.
27.0	Condivisione di gruppi di sicurezza
27.1	Se un gruppo di sicurezza soddisfa questo standard di sicurezza, può essere condiviso tra VPCs lo stesso account e tra account della stessa organizzazione.
27.2	Se un gruppo di sicurezza non soddisfa questo standard e in precedenza era richiesta l'accetta zione del rischio per tale gruppo di sicurezza , l'uso della funzionalità di condivisione dei gruppi di sicurezza tra VPCs lo stesso account o tra account della stessa organizzazione non è consentito senza l'accettazione del rischio per quel nuovo VPC o account.

AMS-STD-X004 - Test di penetrazione

Di seguito è riportato il controllo standard per X004 - Penetration Testing

1. AMS non supporta l'infrastruttura pentest. È responsabilità del cliente. Ad esempio, Kali non è una distribuzione Linux supportata da AMS.

2. I clienti devono attenersi ai test di penetrazione.
3. AMS deve ricevere una notifica preventiva con 24 ore di anticipo nel caso in cui il cliente desideri eseguire test di penetrazione dell'infrastruttura all'interno degli account.
4. AMS fornirà al cliente l'infrastruttura di pentesting in base ai requisiti del cliente esplicitamente indicati nella richiesta di modifica o nella richiesta di assistenza da parte del cliente.
5. La gestione delle identità per l'infrastruttura di pentesting del cliente è responsabilità del cliente.

AMS-STD-X005 - GuardDuty

Di seguito è riportato il controllo standard per X005 - GuardDuty

1. GuardDuty deve essere abilitato in tutti gli account dei clienti in ogni momento.
2. GuardDuty gli avvisi devono essere archiviati nello stesso account o in qualsiasi altro account gestito dalla stessa organizzazione.
3. La funzionalità di elenco IP affidabile di non GuardDuty deve essere utilizzata. In alternativa, è possibile utilizzare l'archiviazione automatica, utile per scopi di controllo.

AMS-STD-X007 - Registrazione

Di seguito è riportato il controllo standard per X007 - Logging

ID	Standard tecnico
1.0	Tipi di registro
1.1	Registri del sistema operativo: tutti gli host devono registrarsi in base al numero minimo di eventi di autenticazione dell'host, eventi di accesso per tutti gli utilizzi di privilegi elevati ed eventi di accesso per tutte le modifiche alla configurazione degli accessi e dei privilegi, comprese quelle relative all'esito positivo e negativo.

ID	Standard tecnico
1.2	AWS CloudTrail: CloudTrail la registrazione degli eventi di gestione deve essere abilitata e configurata per inviare i log a un bucket S3.
1.3	Registri di flusso VPC: tutti i registri del traffico di rete devono essere registrati tramite VPC Flow Logs.
1.4	Amazon S3 Server Access Logging: i bucket S3 obbligatori di AMS che archiviano i log devono avere la registrazione degli accessi al server abilitata.
1.5	AWS Config Istantanee: AWS Config devono registrare le modifiche alla configurazione per tutte le risorse supportate in tutte le regioni e consegnare i file degli snapshot di configura zione ai bucket S3 almeno una volta al giorno.
1,7	Registri delle applicazioni: i clienti possono abilitare la registrazione nelle proprie applicazi oni e archiviarli nel gruppo di log CloudWatch Logs o in un bucket S3.
1.8	Registrazione a livello di oggetto S3: i clienti hanno la possibilità di abilitare la registrazione a livello di oggetto nei propri bucket S3.
1.9	Registrazione dei servizi: i clienti hanno la possibilità di abilitare e inoltrare i log per i servizi SSPS come qualsiasi altro servizio di base.

ID	Standard tecnico
1.10	Log Elastic Load Balancing (Load Classic/Application Load Balancer/Network Balancer): le voci dei log di accesso e degli errori devono essere archiviate nei bucket S3 gestiti da AMS 2.0.
2.0	Controllo degli accessi
2.3	I bucket S3 obbligatori di AMS che archiviano i log non devono consentire l'utilizzo di account di terze parti, come previsto dalle policy relative ai bucket.
2.4	I log dai gruppi di CloudWatch log Logs non devono essere eliminati senza l'approvazione esplicita del contatto di sicurezza autorizzato dal cliente.
3.0	Conservazione dei log
3.1	I gruppi di log CloudWatch Logs obbligatori da AMS devono avere un periodo minimo di conservazione dei log di 90 giorni.
3.2	I bucket S3 obbligatori AMS che archiviano i log devono avere un periodo di conservazione minimo di 18 mesi sui log.
3.3	AWS Backup le istantanee dovrebbero essere disponibili con una conservazione minima di 31 giorni sulle risorse supportate.
4.0	Encryption (Crittografia)
4.1	La crittografia deve essere abilitata in tutti i bucket S3 richiesti da AMS Teams che archivia i log.

ID	Standard tecnico
4.2	Qualsiasi inoltro dei log dagli account dei clienti a qualsiasi altro account deve essere crittogra fato.
5.0	Integrità
5.1	Il meccanismo di integrità dei file di registro deve essere abilitato. Ciò significa configura re la «convalida dei file di registro» negli AWS CloudTrail itinerari richiesti dai team AMS.
6.0	Inoltro dei log
6.1	Qualsiasi registro può essere inoltrato da un account AMS a un altro account AMS dello stesso cliente.
6.2	Qualsiasi registro può essere inoltrato da AMS a un account diverso da AMS solo se l'account non AMS è di proprietà dello stesso cliente AMS (confermando che si tratta dello stesso AWS Organizations account o associando il dominio e-mail al nome dell'azienda del cliente e all'account collegato a PAYER) utilizzando strumenti interni.

Modifiche che introducono rischi di sicurezza elevati o molto elevati nell'ambiente

Le seguenti modifiche introducono un rischio di sicurezza elevato o molto elevato nell'ambiente in uso:

AWS Identity and Access Management

- High_risk-IAM-001: crea chiavi di accesso per l'account root
- high_risk-IAM-002: modifica della politica SCP per consentire accessi aggiuntivi

- high_risk-IAM-003: modifica della politica SCP che potrebbe compromettere l'infrastruttura AMS
- high_risk-IAM-004: creazione di un file role/user con infrastruttura che modifica le autorizzazioni (scrittura, gestione delle autorizzazioni o etichettatura) nell'account del cliente
- high_risk-IAM-005: IAM gestisce le politiche di trust tra account AMS e account di terze parti (non di proprietà del cliente)
- high_risk-IAM-006: politiche interaccount per accedere a qualsiasi chiave KMS da un account AMS tramite un account di terze parti)
- high_risk-IAM-007: politiche tra account di terze parti per accedere al bucket S3 di un cliente AMS o a risorse in cui è possibile archiviare i dati (come Amazon RDS, Amazon DynamoDB o Amazon Redshift)
- high_risk-IAM-008: assegna le autorizzazioni IAM a qualsiasi autorizzazione che modifichi l'infrastruttura nell'account del cliente
- high_risk-IAM-009: consenti l'elenco e la lettura su tutti i bucket S3 dell'account

Sicurezza della rete

- High_risk-NET-001: porte di gestione del sistema operativo aperte SSH/22 o SSH/2222 (non SFTP/2222), TELNET/23, RDP/3389, WinRM/5985-5986, VNC/ 5900-5901 TS/CITRIX/1494 o 1604, LDAP/389 o 636 e NETBIOS/137-139 da Internet
- High_risk-NET-002: porte di gestione del database aperte MySQL/3306, PostgreSQL/5432, Oracle/1521, MSSQL/1433 o qualsiasi porta cliente di gestione da Internet
- High_risk-net-003: apri le porte applicative HTTP/80, HTTPS/8443 e HTTPS/443 direttamente su qualsiasi risorsa di calcolo. Ad esempio, EC2 ECS/EKS/Fargate istanze, contenitori e così via da Internet
- High_risk-net-004: qualsiasi modifica ai gruppi di sicurezza che controllano l'accesso all'infrastruttura AMS
- High_risk-net-006: peering VPC con l'account di terze parti (non di proprietà del cliente)
- High_risk-net-007: aggiunta del firewall del cliente come punto di uscita per tutto il traffico AMS
- High_risk-NET-008: l'allegato Transit Gateway con l'account di terze parti non è consentito
- High_Risk-S3-001: fornisce o abilita l'accesso pubblico nel bucket S3

Registrazione di log

- CloudTrailHigh_risk-log-001: disabilita.

- High_risk-log-002: disabilita i registri di flusso VPC.
- High_risk-log-003: inoltro dei log tramite qualsiasi metodo (notifica di eventi S3, pull dell'agente SIEM, push dell'agente SIEM ecc.) da un account gestito da AMS a un account di terze parti (non di proprietà del cliente)
- High_risk-log-004: utilizza percorsi non AMS per CloudTrail

Miscellaneous (Varie)

- High_risk-ENC-001: disabilita la crittografia in qualsiasi risorsa se è abilitata

Domande frequenti sulla sicurezza

AMS fornisce assistenza 24 ore su 24, 7 giorni su 7, 365 giorni follow-the-sun l'anno tramite centri operativi globali. I tecnici operativi AMS dedicati monitorano attivamente i dashboard e le code degli incidenti. Di solito, AMS gestisce i tuoi account tramite l'automazione. In rare circostanze che richiedono competenze specifiche in materia di risoluzione dei problemi o di implementazione, un tecnico operativo AMS potrebbe accedere ai vostri AWS account.

Di seguito sono riportate le domande più comuni sulle migliori pratiche di sicurezza, i controlli, i modelli di accesso e i meccanismi di controllo che AMS Accelerate utilizza quando un tecnico operativo o un addetto all'automazione di AMS accede ai vostri account.

Quando gli ingegneri operativi AMS accedono ai miei ambienti?

I tecnici operativi AMS non hanno accesso permanente ai tuoi account o alle tue istanze. L'accesso agli account dei clienti è concesso agli operatori AMS solo per casi d'uso aziendali giustificabili, come avvisi, incidenti, richieste di modifica e così via. L'accesso è documentato nei log. AWS CloudTrail

Per la giustificazione dell'accesso, i trigger e gli iniziatori dei trigger, vedere. Trigger di accesso all'account cliente AMS

Quali ruoli assumono i tecnici operativi di AMS quando accedono ai miei account?

Nei rari casi (~ 5%) che richiedono l'intervento umano nell'ambiente, i tecnici operativi AMS accedono al tuo account con un ruolo di accesso predefinito in sola lettura. Il ruolo predefinito non ha accesso a nessun contenuto comunemente archiviato negli archivi di dati, come Amazon Simple Storage

Service, Amazon Relational Database Service, Amazon DynamoDB, Amazon Redshift e Amazon. ElastiCache

Per un elenco dei ruoli necessari ai tecnici operativi e ai sistemi AMS per fornire servizi nel tuo account, consulta. Ruoli IAM di accesso all'account cliente AMS

In che modo un tecnico operativo AMS accede al mio account?

Per accedere agli account dei clienti, i tecnici operativi AMS utilizzano un servizio di accesso AMS AWS interno. Questo servizio interno è disponibile solo attraverso un canale privato e sicuro, in modo che l'accesso ai tuoi account sia sicuro e controllato.

1. I tecnici operativi AMS utilizzano l'autenticazione interna del servizio di accesso AMS insieme a un'autenticazione a due fattori. Inoltre, il tecnico operativo deve fornire una giustificazione aziendale (ticket relativo all'incidente o ID della richiesta di assistenza) che dimostri la necessità di accedere all'account. AWS
2. In base all'autorizzazione del tecnico operativo, il servizio di accesso AMS fornisce all'ingegnere il ruolo appropriato (Read-only/Operator/Admin) e l'URL di accesso alla console AWS . L'accesso al tuo account è di breve durata e limitato nel tempo.
3. Per accedere alle istanze Amazon EC2, i tecnici operativi AMS utilizzano lo stesso servizio di accesso AMS interno del broker. Una volta concesso l'accesso, i tecnici operativi AMS accedono AWS Systems Manager Session Manager alle istanze con credenziali di sessione di breve durata.

   Per fornire l'accesso RDP per le istanze Windows, il tecnico operativo utilizza Amazon EC2 Systems Manager per creare un utente locale sull'istanza e stabilire il port forwarding verso l'istanza. L'ingegnere operativo utilizza le credenziali utente locali per l'accesso RDP all'istanza. Le credenziali dell'utente locale vengono rimosse alla fine della sessione.

Il diagramma seguente illustra il processo utilizzato dai tecnici operativi AMS per accedere all'account:

Come posso tenere traccia delle modifiche apportate da AMS nei miei AWS account gestiti da AMS?

Accesso all'account

Per aiutarti a tenere traccia delle modifiche apportate dall'automazione o dal team operativo di AMS Accelerate, AMS fornisce l'interfaccia SQL Change record nella console Amazon Athena e i log AMS Accelerate. Queste risorse forniscono le seguenti informazioni:

- Chi ha avuto accesso al tuo account.
- Quando è stato effettuato l'accesso all'account.
- Quali privilegi sono stati utilizzati per accedere al tuo account.
- Quali modifiche sono state apportate da AMS Accelerate al tuo account.
- Perché sono state apportate le modifiche al tuo account.

Configurazione delle risorse

Visualizza CloudTrail i log per tenere traccia delle configurazioni AWS delle tue risorse negli ultimi 90 giorni. Se la tua configurazione risale a più di 90 giorni, accedi ai log in Amazon S3.

Registri delle istanze

Amazon CloudWatch Agent raccoglie i log del sistema operativo. Visualizza CloudWatch i log per vedere i log di accesso e di altre azioni supportati dal tuo sistema operativo.

Per ulteriori informazioni, consulta Monitoraggio delle modifiche nei tuoi account AMS Accelerate.

Quali sono i controlli di processo per l'accesso dei tecnici operativi AMS al mio account?

Prima di entrare in AMS, gli ingegneri operativi vengono sottoposti a un controllo dei precedenti penali. Poiché gli ingegneri AMS gestiscono l'infrastruttura dei clienti, hanno anche un controllo annuale obbligatorio dei precedenti. Se un tecnico non supera il controllo dei precedenti, l'accesso viene revocato.

Tutti i tecnici operativi di AMS devono completare la formazione obbligatoria sulla sicurezza, ad esempio sulla sicurezza dell'infrastruttura, la sicurezza dei dati e la risposta agli incidenti prima di poter accedere alle risorse.

Come viene gestito l'accesso privilegiato?

Un sottoinsieme di utenti deve completare una formazione aggiuntiva e mantenere i diritti di accesso privilegiati per un accesso elevato. L'accesso e l'utilizzo vengono ispezionati e controllati. AMS limita

l'accesso privilegiato a circostanze eccezionali o quando l'accesso con privilegio minimo non è in grado di soddisfare la richiesta. L'accesso privilegiato è inoltre limitato nel tempo.

I tecnici operativi di AMS utilizzano l'MFA?

Sì. Tutti gli utenti devono utilizzare MFA e Proof of Presence per fornirti servizi.

Cosa succede al loro accesso quando un dipendente AMS lascia l'organizzazione o cambia ruolo lavorativo?

L'accesso agli account e alle risorse dei clienti viene fornito tramite l'appartenenza al gruppo interno. L'iscrizione si basa su criteri rigorosi, tra cui lo specifico ruolo professionale, il responsabile dei rapporti e lo status occupazionale in AMS. Se la famiglia professionale di un tecnico operativo cambia o il suo ID utente viene disabilitato, l'accesso viene revocato.

Quali controlli di accesso regolano l'accesso dei tecnici operativi AMS ai miei account?

Esistono diversi livelli di controlli tecnici per far rispettare i principi di «necessità di sapere» e «privilegio minimo» per l'accesso all'ambiente. Di seguito è riportato un elenco dei controlli di accesso:

- Tutti i tecnici operativi devono far parte di uno specifico AWS gruppo interno per accedere agli account e alle risorse dei clienti. L'appartenenza al gruppo è strettamente basata sulla necessità di conoscere ed è automatizzata con criteri predefiniti.
- AMS pratica l'accesso «non persistente» all'ambiente. Ciò significa che l'accesso ai vostri AWS account da parte delle operazioni AMS avviene "just-in-time" con credenziali di breve durata. L'accesso agli account viene fornito solo dopo l'invio e la verifica di una giustificazione interna del business case (richiesta di assistenza, incidente, richiesta di gestione delle modifiche e così via).
- AMS segue il principio del privilegio minimo. Pertanto, i tecnici operativi autorizzati presuppongono l'accesso in sola lettura per impostazione predefinita. L'accesso in scrittura viene utilizzato dai tecnici solo quando sono necessarie modifiche all'ambiente a causa di un incidente o di una richiesta di modifica.
- AMS utilizza AWS Identity and Access Management ruoli standard facilmente identificabili che utilizzano il prefisso «ams» per monitorare e gestire gli account. Tutti gli accessi vengono registrati AWS CloudTrail per consentirti di verificarli.

- AMS utilizza strumenti di backend automatizzati per rilevare le modifiche non autorizzate all'account durante la fase di convalida delle informazioni sui clienti durante la fase di esecuzione delle modifiche.

In che modo AMS monitora l'accesso degli utenti root?

L'accesso root attiva sempre il processo di risposta agli incidenti. AMS utilizza il GuardDuty rilevamento di Amazon per monitorare l'attività degli utenti root. Se GuardDuty genera un avviso, AMS crea un evento per ulteriori indagini. AMS ti avvisa se viene rilevata un'attività imprevista dell'account root e il team di sicurezza di AMS avvia un'indagine.

In che modo AMS risponde agli incidenti di sicurezza?

AMS analizza gli eventi di sicurezza generati da servizi di rilevamento come Amazon GuardDuty, Amazon Macie e dai problemi di sicurezza segnalati dai clienti. AMS collabora con il vostro team di risposta alla sicurezza per eseguire il processo Security Incident Response (SIR). Il processo AMS SIR si basa sul framework NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide e fornisce una risposta di sicurezza 24 ore su 24, 365 giorni all'anno. follow-the-sun AMS collabora con te per analizzare e contenere rapidamente gli incidenti di sicurezza.

A quali certificazioni e framework standard del settore aderisce AMS?

Come altri AWS servizi, AWS Managed Services è certificato per OSPAR, HIPAA, HITRUST, GDPR, SOC*, ISO*, FedRAMP (Medium/High), IRAP e PCI. Per ulteriori informazioni sulle certificazioni di conformità dei clienti, sui regolamenti e sui framework a cui si AWS allinea, consulta AWS Compliance.

Barriere di sicurezza

AWS Managed Services utilizza più controlli per proteggere le tue risorse informative e aiutarti a mantenere sicura la tua AWS infrastruttura. AMS Accelerate mantiene una libreria di AWS Config regole e azioni correttive per aiutarti a garantire che i tuoi account siano conformi agli standard di settore per la sicurezza e l'integrità operativa. AWS Config le regole tengono costantemente traccia delle modifiche alla configurazione delle risorse registrate. Se una modifica viola le condizioni di una regola, AMS te ne segnala i risultati. Puoi porre rimedio alle violazioni automaticamente o su richiesta, in base alla gravità della violazione.

AMS utilizza AWS Config regole per contribuire a soddisfare i requisiti dei seguenti standard:

- Centro per la sicurezza in Internet (CIS)
- Framework di sicurezza cloud (CSF) del National Institute of Standards and Technology (NIST)
- Health Insurance Portability and Accountability Act (HIPAA)
- Standard di sicurezza dei dati (DSS) del settore delle carte di pagamento (PCI)

Per ulteriori informazioni, consulta Gestione della sicurezza in AMS Accelerate

Come posso accedere ai report più recenti sulla certificazione di sicurezza, sui framework e sulla conformità in materia? AWS

È possibile trovare i report di sicurezza e conformità correnti per AWS i servizi utilizzando i seguenti metodi:

- È possibile utilizzare AWS Artifactper scaricare il rapporto più recente sulla sicurezza, la disponibilità e la riservatezza di un AWS servizio.
- Per un elenco della maggior parte dei AWS servizi, incluso AWS Managed Services, conformi ai framework di conformità globali, consulta. https://aws.amazon.com/compliance/services-in-scope/ Ad esempio, seleziona PCI e cerca AWS Managed Services.

  Puoi cercare «AMS» per trovare elementi di sicurezza specifici per AMS da un account gestito da AMS. AWS AWS Managed Services rientra nell'ambito del SOC 3.
- Il rapporto AWS SOC 2 (System and Organizations Controls) viene pubblicato nel AWS Artifact repository. Questo rapporto valuta i AWS controlli che soddisfano i criteri di sicurezza, disponibilità e riservatezza stabiliti nella sezione 100 del TSP dell'American Institute of Certified Public Accountants (AICPA), Trust Services Criteria.

AMS condivide diagrammi di architettura di riferimento relativi a diversi aspetti delle funzionalità di AMS?

Per visualizzare l'architettura di riferimento AMS, scarica il PDF di AWS Managed Services for Proactive Monitoring.

In che modo AMS monitora chi accede ai miei account e quali sono le esigenze aziendali di accesso?

Per supportare la continuità del servizio e la sicurezza degli account, AMS accede all'account o alle istanze solo in risposta a eventi proattivi relativi a salute o manutenzione, salute o sicurezza, attività pianificate o richieste dei clienti. L'accesso ai tuoi account è autorizzato tramite i processi AMS, come indicato nel modello di accesso per AMS Accelerate. Questi flussi di autorizzazione contengono barriere per impedire accessi involontari o inappropriati. Come parte del flusso di accesso, AMS fornisce al sistema di autorizzazione le esigenze aziendali. Questa esigenza aziendale potrebbe essere un elemento di lavoro associato al tuo account, ad esempio un caso che hai aperto con AMS. In alternativa, l'esigenza aziendale potrebbe essere un flusso di lavoro autorizzato, come la soluzione Patching. Tutti gli accessi richiedono una giustificazione convalidata, verificata e autorizzata in tempo reale dai sistemi AMS interni sulla base di regole aziendali per allineare le richieste di accesso a un'esigenza aziendale.

Ai tecnici operativi di AMS non viene fornito un percorso per accedere ai tuoi account senza esigenze aziendali valide. Tutti gli accessi all'account e le esigenze aziendali associate vengono assegnati alle AWS CloudTrail voci all'interno AWS dei vostri account. Ciò garantisce la massima trasparenza e l'opportunità di effettuare verifiche e ispezioni in modo autonomo. Oltre all'ispezione, AMS dispone di ispezioni automatizzate ed esegue l'ispezione manuale, se necessario, delle richieste di accesso ed esegue verifiche degli strumenti e dell'accesso umano per esaminare gli accessi anomali.

I tecnici AMS hanno accesso ai miei dati archiviati in servizi di archiviazione AWS dati, come Amazon S3, Amazon RDS, DynamoDB e Amazon Redshift?

I tecnici AMS non hanno accesso ai contenuti dei clienti archiviati nei AWS servizi comunemente utilizzati per l'archiviazione dei dati. L'accesso ai dati AWS APIs utilizzati per leggere, scrivere, modificare o eliminare in questi servizi è limitato da una politica di negazione esplicita di IAM associata ai ruoli IAM utilizzati per l'accesso degli ingegneri AMS. Inoltre, i guardrail e le automazioni interne di AMS impediscono ai tecnici operativi di AMS di rimuovere o modificare le condizioni di negazione.

I tecnici AMS hanno accesso ai dati dei clienti archiviati in Amazon EBS, Amazon EFS e Amazon FSx?

I tecnici AMS possono accedere alle istanze Amazon EC2 come amministratori. L'accesso da amministratore è necessario per la risoluzione di alcuni scenari che includono, a titolo esemplificativo, problemi del sistema operativo (OS) e guasti delle patch. Gli ingegneri AMS in genere accedono al volume di sistema per risolvere i problemi rilevati. Tuttavia, l'accesso per gli ingegneri AMS non è limitato o limitato al volume del sistema.

In che modo l'accesso viene limitato o controllato per i ruoli di automazione che dispongono di privilegi elevati per i miei ambienti?

Il `ams-access-admin` ruolo viene utilizzato esclusivamente dall'automazione AMS. Queste automazioni implementano, gestiscono e mantengono le risorse necessarie utilizzate da AMS per l'implementazione nei vostri ambienti per la raccolta di dati di telemetria, salute e sicurezza per lo svolgimento delle funzioni operative. Gli ingegneri AMS non possono assumere ruoli di automazione e sono limitati dalla mappatura dei ruoli nei sistemi interni. In fase di esecuzione, AMS applica dinamicamente una politica di sessione con privilegi minimi e ristretti a ogni automazione. Questa politica di sessione limita la capacità e le autorizzazioni dell'automazione.

In che modo AMS implementa il principio del privilegio minimo come richiesto nel AWS Well-Architected Framework per i ruoli di automazione?

In fase di esecuzione, AMS applica una politica di sessione ristretta con privilegi minimi a ogni automazione. Questa politica di sessione ristretta limita la capacità e le autorizzazioni dell'automazione. Le policy di sessione che dispongono delle autorizzazioni per creare risorse IAM richiedono anche l'aggiunta di un limite di autorizzazione. Questo limite di autorizzazione riduce il rischio di escalation dei privilegi. Ogni team adotta una politica di sessione utilizzata solo da quel team.

Quali sistemi di registrazione e monitoraggio vengono utilizzati per rilevare tentativi di accesso non autorizzati o attività sospette che coinvolgono ruoli di automazione?

AWS mantiene archivi centralizzati che forniscono le principali funzionalità di archiviazione dei log per uso interno da parte dei team di assistenza. AWS Questi log sono archiviati in Amazon S3 per

garantire scalabilità, durabilità e disponibilità elevate. AWS I team di assistenza possono quindi raccogliere, archiviare e visualizzare i registri di servizio in un servizio di registro centrale.

Gli host di produzione AWS vengono distribuiti utilizzando immagini di base principali. Le immagini di base sono dotate di un set standard di configurazioni e funzioni che includono la registrazione e il monitoraggio per scopi di sicurezza. Questi registri vengono archiviati e accessibili dai team di AWS sicurezza per l'analisi delle cause principali in caso di sospetto incidente di sicurezza.

I log di un determinato host sono disponibili per il team proprietario di quell'host. I team possono cercare nei propri log per analisi operative e di sicurezza.

Come vengono gestiti gli incidenti o le violazioni di sicurezza riguardanti l'infrastruttura di automazione e quali protocolli aiutano a rispondere e mitigare rapidamente?

AWS i piani di emergenza e i playbook di risposta agli incidenti hanno definito e testato strumenti e processi per rilevare, mitigare, indagare e valutare gli incidenti di sicurezza. Questi piani e playbook includono linee guida per rispondere a potenziali violazioni dei dati in conformità ai requisiti contrattuali e normativi.

Vengono effettuati regolarmente valutazioni di sicurezza, scansioni di vulnerabilità e test di penetrazione sull'infrastruttura di automazione?

AWS Security esegue regolarmente scansioni di vulnerabilità sui sistemi operativi host, sulle applicazioni Web e sui database AWS dell'ambiente utilizzando una varietà di strumenti. AWS I team di sicurezza si abbonano inoltre ai feed di notizie per individuare eventuali difetti dei fornitori e monitorano in modo proattivo i siti Web dei fornitori e altri punti vendita pertinenti alla ricerca di nuove patch.

In che modo l'accesso all'infrastruttura di automazione è limitato solo al personale autorizzato?

L'accesso ai AWS sistemi viene assegnato in base al privilegio minimo e approvato da un individuo autorizzato. I compiti e le aree di responsabilità (ad esempio, richiesta e approvazione dell'accesso, richiesta e approvazione della gestione delle modifiche, sviluppo delle modifiche, test e implementazione e così via) sono suddivisi tra diversi soggetti per ridurre le modifiche o l'uso improprio non autorizzati o involontari dei sistemi. AWS Gli account di gruppo o condivisi non sono consentiti all'interno dei confini del sistema.

Quali misure vengono implementate per mantenere gli standard di sicurezza e prevenire accessi non autorizzati o violazioni dei dati nella pipeline di automazione?

L'accesso alle risorse, inclusi servizi, host, dispositivi di rete e gruppi Windows e UNIX, viene approvato nel sistema di gestione delle autorizzazioni AWS proprietario dal proprietario o dal gestore appropriato. Il registro dello strumento di gestione delle autorizzazioni registra le richieste di modifiche di accesso. Le modifiche alle funzioni lavorative revocano automaticamente l'accesso del dipendente alle risorse. L'accesso continuo per quel dipendente deve essere richiesto e approvato.

AWS richiede l'autenticazione a due fattori su un canale crittografico approvato per l'autenticazione alla AWS rete interna da postazioni remote. I dispositivi firewall limitano l'accesso all'ambiente informatico, impongono i confini dei cluster di elaborazione e limitano l'accesso alle reti di produzione.

Vengono implementati processi per proteggere le informazioni e gli strumenti di controllo da accessi, modifiche ed eliminazioni non autorizzati. I registri di audit contengono una serie di elementi di dati per supportare i requisiti di analisi necessari. Inoltre, i registri di audit sono disponibili per gli utenti autorizzati per l'ispezione o l'analisi su richiesta e in risposta a eventi relativi alla sicurezza o che hanno un impatto sull'azienda.

I diritti di accesso degli utenti ai AWS sistemi (ad esempio, rete, applicazioni, strumenti, ecc.) vengono revocati entro 24 ore dalla cessazione o dalla disattivazione. Gli account utente inattivi vengono disabilitati e and/or rimossi almeno ogni 90 giorni.

Il rilevamento o il monitoraggio delle anomalie sono attivati per l'accesso o la registrazione degli audit per rilevare l'aumento dei privilegi o l'uso improprio degli accessi per avvisare in modo proattivo il team AMS?

Gli host di produzione di AWS sono dotati di registrazione per motivi di sicurezza. Questo servizio registra le azioni umane sugli host, inclusi gli accessi, i tentativi di accesso non riusciti e le disconnessioni. Questi registri vengono archiviati e accessibili dai team AWS di sicurezza per l'analisi della causa principale in caso di sospetto incidente di sicurezza. I log di un determinato host sono disponibili anche per il team proprietario di quell'host. I team di assistenza hanno a disposizione uno strumento di analisi dei log front-end per effettuare ricerche nei log per analisi operative e di sicurezza. Vengono implementati processi per proteggere i log e gli strumenti di controllo da accessi, modifiche ed eliminazioni non autorizzati. Il team AWS di sicurezza esegue l'analisi dei registri per identificare gli eventi sulla base di parametri di gestione del rischio definiti.

Quali tipi di dati dei clienti vengono estratti dagli account gestiti da AMS e come vengono utilizzati e archiviati?

AMS non accede né utilizza i tuoi contenuti per nessuno scopo. AMS definisce i contenuti dei clienti come software (comprese le immagini delle macchine), dati, testo, audio, video o immagini su cui un cliente o qualsiasi utente finale trasferisce AWS per l'elaborazione, l'archiviazione o l'hosting Servizi AWS in relazione all'account del cliente, e qualsiasi risultato computazionale che un cliente o il suo utente finale ricava da quanto precede attraverso il loro utilizzo. Servizi AWS

Monitoraggio e gestione degli eventi in AMS Accelerate

Il sistema di monitoraggio AMS Accelerate monitora AWS le tue risorse per individuare guasti, peggioramento delle prestazioni e problemi di sicurezza.

In qualità di account gestito, AMS Accelerate configura e implementa allarmi per le AWS risorse applicabili, monitora tali risorse ed esegue le riparazioni quando necessario.

Il sistema di monitoraggio AMS Accelerate si basa su strumenti interni, come Resource Tagger e Alarm Manager Servizi AWS, e sfrutta AWS AppConfigAmazon CloudWatch ()CloudWatch, Amazon EventBridge (precedentemente noto come) CloudWatch, Amazon, Amazon GuardDuty Macie e. AWS Health

AMS Accelerate offre una gamma di servizi operativi per aiutarti a raggiungere l'eccellenza operativa su. AWSPer comprendere rapidamente come AMS aiuta i team a raggiungere l'eccellenza operativa complessiva Cloud AWS grazie ad alcune delle nostre funzionalità operative chiave, tra cui l'helpdesk 24 ore su 24, 7 giorni su 7, il monitoraggio proattivo, la sicurezza, l'applicazione di patch, la registrazione e il backup, consulta i diagrammi dell'architettura di riferimento di AMS.

Argomenti

- Che cos'è il monitoraggio?
- Come funziona il monitoraggio
- Avvisi dal monitoraggio di base in AMS
- Notifiche di incidenti con riconoscimento delle applicazioni in AMS
- Accelera Alarm Manager
- Correzione automatica degli avvisi con AMS
- Utilizzo di Amazon EventBridge Managed Rules in AMS
- Trusted Remediator in AMS

Per informazioni sul monitoraggio di Amazon EKS, consulta Monitoraggio e gestione degli incidenti per Amazon EKS in AMS Accelerate

Che cos'è il monitoraggio?

Il monitoraggio di AMS Accelerate offre i seguenti vantaggi:

- Una configurazione predefinita che crea, gestisce e implementa politiche nell'account gestito per tutte le AWS risorse o supportate selezionate.
- Una linea di base di monitoraggio in modo da avere un livello di protezione predefinito, anche se non configuri nessun altro monitoraggio per i tuoi account gestiti. Per ulteriori informazioni, consulta Avvisi dal monitoraggio di base in AMS.
- La possibilità di personalizzare gli allarmi relativi alle risorse di base per soddisfare le vostre esigenze.
- Correzione automatica degli avvisi da parte di AMS Operations, quando possibile, per prevenire o ridurre l'impatto sulle applicazioni. Ad esempio, se utilizzi un' EC2 istanza Amazon autonoma che non supera il controllo dello stato del sistema, AMS tenta di ripristinare l'istanza interrompendola e riavviandola. Per ulteriori informazioni, consulta Correzione automatica degli avvisi con AMS.
- Visibilità degli avvisi attivi e risolti in precedenza utilizzando. OpsCenter Ad esempio, se hai un utilizzo imprevisto elevato della CPU su un' EC2 istanza Amazon, puoi richiedere l'accesso alla AWS Systems Manager console (che include l'accesso alla OpsCenter console) e visualizzarla OpsItem direttamente nella OpsCenter console.
- Analisi degli avvisi per determinare le azioni appropriate. Per ulteriori informazioni, consulta Gestione degli incidenti in AMS Accelerate.
- Avvisi generati in base alla configurazione dell'account e ai servizi supportati. AWS La configurazione di monitoraggio di un account si riferisce a tutti i parametri delle risorse dell'account che creano un avviso. La configurazione di monitoraggio di un account include le definizioni di CloudWatch allarme e EventBridge (precedentemente noti come CloudWatch Eventi) che generano l'avviso (allarme o evento). Per ulteriori informazioni sui parametri delle risorse, vedere. Avvisi dal monitoraggio di base in AMS
- Notifica di guasti imminenti, in corso, ricorrenti o potenziali, peggioramento delle prestazioni o problemi di sicurezza generati dal monitoraggio di base configurato in un account (noto come avviso). Esempi di avvisi includono un CloudWatch allarme, un evento o un risultato proveniente da un servizio, ad esempio o. AWS GuardDuty AWS Health

Come funziona il monitoraggio

Guarda la seguente grafica sull'architettura di monitoraggio in AWS Managed Services (AMS).

Il diagramma seguente illustra l'architettura di monitoraggio AMS Accelerate.

Dopo aver etichettato le risorse in base alla politica definita utilizzando Resource tagger e implementate le definizioni degli allarmi, l'elenco seguente descrive i processi di monitoraggio AMS.

- Generazione: al momento dell'onboarding dell'account, AMS configura il monitoraggio di base (una combinazione di allarmi CloudWatch (CW) e regole degli eventi CW) per tutte le risorse create in un account gestito. La configurazione di monitoraggio di base genera un avviso quando viene attivato un allarme CW o viene generato un evento CW.
- Aggregazione: tutti gli avvisi generati dalle tue risorse vengono inviati al sistema di monitoraggio AMS indirizzandoli a un argomento SNS dell'account. Puoi anche configurare il modo in cui AMS raggruppa gli avvisi di Amazon EC2. AMS raggruppa tutti gli avvisi relativi alla stessa istanza EC2 in un unico incidente o crea un incidente per avviso, a seconda delle preferenze. Puoi modificare questa configurazione in qualsiasi momento collaborando con il tuo Cloud Service Delivery Manager o Cloud Architect.
- Elaborazione: AMS analizza gli avvisi e li elabora in base al loro potenziale impatto. Gli avvisi vengono elaborati come descritto di seguito.
  - Avvisi con impatto noto sui clienti: portano alla creazione di un nuovo rapporto sugli incidenti e AMS segue il processo di gestione degli incidenti.

    Esempio di avviso: un'istanza Amazon EC2 non supera un controllo dello stato del sistema, AMS tenta di ripristinare l'istanza interrompendola e riavviandola.
  - Avvisi con un impatto incerto sui clienti: per questi tipi di avvisi, AMS invia un rapporto sugli incidenti, in molti casi chiedendo di verificare l'impatto prima che AMS intervenga. Tuttavia, se i controlli relativi all'infrastruttura vengono superati, AMS non ti invia una segnalazione sull'incidente.

    Ad esempio: un avviso per un utilizzo della CPU superiore all'85% per più di 10 minuti su un'istanza Amazon EC2 non può essere immediatamente classificato come incidente poiché questo comportamento potrebbe essere previsto in base all'utilizzo. In questo esempio, AMS Automation esegue controlli relativi all'infrastruttura sulla risorsa. Se tali controlli vengono superati, AMS non invia una notifica di avviso, anche se l'utilizzo della CPU supera il 99%. Se Automation rileva che i controlli relativi all'infrastruttura non riescono sulla risorsa, AMS invia una notifica di avviso e verifica se è necessaria una mitigazione. Le notifiche di avviso sono descritte in dettaglio in questa sezione. AMS offre opzioni di mitigazione nella notifica. Quando rispondi alla notifica confermando che l'avviso è un incidente, AMS crea un nuovo rapporto sull'incidente e inizia il processo di gestione degli incidenti AMS. Le notifiche di servizio che ricevono una risposta di «nessun impatto sul cliente» o nessuna risposta per tre giorni, vengono contrassegnate come risolte e l'avviso corrispondente viene contrassegnato come risolto.

- Avvisi senza impatto sul cliente: se, dopo la valutazione, AMS determina che l'avviso non ha alcun impatto sul cliente, l'avviso viene chiuso.

  Ad esempio, AWS Health notifica la presenza di un'istanza EC2 che richiede la sostituzione, ma da allora tale istanza è stata interrotta.

Notifiche raggruppate di istanze EC2

Puoi configurare il monitoraggio AMS per raggruppare gli avvisi provenienti dalla stessa istanza EC2 in un unico incidente. Il tuo Cloud Service Delivery Manager o Cloud Architect può configurarlo per te. È possibile configurare quattro parametri per ogni account gestito da AMS.

1. Ambito: scegli a livello di account o basato su tag.
   - Per specificare una configurazione applicabile a ogni istanza EC2 di quell'account, scegli scope = account-wide.
   - Per specificare una configurazione che si applichi solo alle istanze EC2 di quell'account con un tag specifico, scegli scope = tag-based.
2. Regola di raggruppamento : scegli la versione classica o l'istanza.
   - Per configurare il raggruppamento a livello di istanza per ogni risorsa del tuo account, scegli ambito = a livello di account e regola di raggruppamento = istanza.
   - Per configurare risorse specifiche nel tuo account per utilizzare il raggruppamento a livello di istanza, tagga tali istanze e quindi scegli scope = basato su tag e regola di raggruppamento = livello di istanza.
   - Per non utilizzare il raggruppamento di istanze per gli avvisi nel tuo account, scegli la regola di raggruppamento = classica.
3. Opzione di coinvolgimento: scegli nessuna opzione, solo report o predefinita.
   - Affinché AMS non crei incidenti o non esegua automazioni per gli allarmi utilizzando tali risorse mentre la configurazione è attiva, scegli nessuna.
   - Affinché AMS non crei incidenti o esegua automazioni per gli allarmi da tali risorse mentre la configurazione è attiva e non esegua documenti di correzione automatica di Systems Manager, ma per includere i record di questi eventi nei report, scegli solo report. Ciò può essere utile se desiderate ridurre il volume dei casi di assistenza in caso di incidenti con cui interagite e se alcuni incidenti causati da alcune risorse non richiedono un'attenzione immediata, ad esempio quelli relativi a un account non di produzione.

- Affinché AMS elabori gli avvisi, esegua automazioni e crei casi di incidenti quando necessario, scegli Default.

4. Risolvi dopo: scegli tra 24 ore, 48 ore o 72 ore. Infine, configura quando i casi di incidente vengono chiusi automaticamente. Se l'ora dell'ultima corrispondenza tra i casi raggiunge il valore Resolve after configurato, l'incidente viene chiuso.

Notifica di avviso

Come parte dell'elaborazione degli avvisi, basata sull'analisi dell'impatto, AWS Managed Services (AMS) crea un incidente e avvia il processo di gestione degli incidenti per la correzione, quando è possibile determinare l'impatto. Se non è possibile determinare l'impatto, AMS invia una notifica di avviso all'indirizzo e-mail associato al tuo account tramite una notifica di servizio. In alcuni scenari, questa notifica di avviso non viene inviata. Ad esempio, se i controlli relativi all'infrastruttura vengono superati per un avviso di utilizzo elevato della CPU, all'utente non viene inviata una notifica di avviso. Per ulteriori informazioni, consulta il diagramma sull'architettura di monitoraggio AMS per il processo di gestione degli avvisi in. Come funziona il monitoraggio

Notifica di avviso basata su tag

Utilizza i tag per inviare notifiche di avviso relative alle tue risorse a diversi indirizzi e-mail. È consigliabile utilizzare notifiche di avviso basate su tag, poiché le notifiche inviate a un singolo indirizzo e-mail potrebbero creare confusione quando più team di sviluppatori utilizzano lo stesso account. Le notifiche di avviso basate su tag non sono influenzate dalle Notifiche raggruppate di istanze EC2 impostazioni scelte.

Con le notifiche di avviso basate su tag puoi:

- Inviare avvisi a un indirizzo e-mail specifico: contrassegna le risorse che dispongono di avvisi che devono essere inviati a un indirizzo e-mail specifico con,. `key = OwnerTeamEmail` `value = EMAIL_ADDRESS`
- Invia avvisi a più indirizzi e-mail: per utilizzare più indirizzi e-mail, specifica un elenco di valori separati da virgole. Ad esempio, `key = OwnerTeamEmail`, `value = EMAIL_ADDRESS_1, EMAIL_ADDRESS_2, EMAIL_ADDRESS_3, ...`. Il numero totale di caratteri per il campo del valore non può superare 260.
- Usa una chiave di tag personalizzata: per utilizzare una chiave di tag personalizzata, fornisci il nome della chiave tag personalizzata al tuo CSDM in un'e-mail che dia esplicitamente il consenso

all'attivazione di notifiche automatiche per la comunicazione basata su tag. È consigliabile utilizzare la stessa strategia di tagging per i tag di contatto in tutte le istanze e le risorse.

> **Note**
>
> Il valore chiave `OwnerTeamEmail` non deve necessariamente essere nel caso di camel. Tuttavia, i tag fanno distinzione tra maiuscole e minuscole ed è consigliabile utilizzare il formato consigliato.
> L'indirizzo e-mail deve essere specificato per intero, con il segno «at» (@) per separare la parte locale dal dominio. Esempi di indirizzi e-mail non validi: `Team.AppATabc.xyz` o`john.doe`. Per indicazioni generali sulla tua strategia di tagging, consulta AWS Tagging resources. Non aggiungere informazioni di identificazione personale (PII) nei tag. Usa liste di distribuzione o alias laddove possibile.
> La notifica di avviso basata su tag è supportata per le risorse dei seguenti Amazon Services: EC2, Elastic Block Store (EBS), Elastic Load Balancing (ELB), Application Load Balancer (ALB), Network Load Balancer, Relational Database Service (RDS), Elastic File System (EFS), e VPN OpenSearch. FSx Site-to-Site

Avvisi dal monitoraggio di base in AMS

Scopri le impostazioni predefinite di monitoraggio di AMS Accelerate. Per ulteriori informazioni, consulta Monitoraggio e gestione degli eventi in AMS Accelerate.

La tabella seguente mostra cosa viene monitorato e le soglie di allarme predefinite. È possibile modificare le soglie di avviso con un documento di configurazione personalizzato o inviare una richiesta di servizio. Per istruzioni su come modificare la configurazione personalizzata degli allarmi, consulta. Modifica della configurazione dell'allarme Accelerate Per ricevere notifiche quando gli allarmi superano la soglia, oltre alla procedura di avviso standard di AMS, puoi sovrascrivere le configurazioni degli allarmi. Per istruzioni, consulta Accelera Alarm Manager.

Amazon CloudWatch offre una conservazione estesa dei parametri. Per ulteriori informazioni, consulta CloudWatch Limiti.

> **Note**
>
> AMS Accelerate calibra il monitoraggio di base su base periodica. L'onboarding di nuovi account viene sempre effettuato con il monitoraggio di base più recente e la tabella descrive il

monitoraggio di base per un account che ha appena effettuato l'onboarding. AMS Accelerate aggiorna periodicamente il monitoraggio di base negli account esistenti e potrebbe verificarsi un ritardo prima che gli aggiornamenti siano operativi.

Avvisi provenienti dal monitoraggio di base

Tipo di servizio/risorsa	Fonte dell'avviso e condizione di attivazione	Nome e note dell'avviso
Per gli avvisi contrassegnati da un asterisco (*), AMS valuta in modo proattivo l'impatto e corregge quando possibile; se la correzione non è possibile, AMS crea un incidente. Nel caso in cui l'automazione non riesca a risolvere il problema, AMS informa l'utente del caso in cui si è verificat o l'incidente e viene assunto un tecnico AMS. Inoltre, se accedi all'argomento Direct-Customer-Al erts SNS, questi avvisi vengono inviati direttamente alla tua e-mail.		
Istanza di Application Load Balancer	ApplicationLoadBalancerErro rCount (HTTPCode_ELB_5XX_Count/ RequestCount) *100 somma > 15% per 1 minuto, 5 volte consecutive.	Conteggio degli errori LoadBalancer HTTP 5XX dell'applicazione CloudWatch allarme relativo al numero eccessivo di codici di risposta HTTP 5XX generati dal Loadbalancer.
Istanza di Application Load Balancer	RejectedConnectionCount somma > 0% per 1 minuto, 5 volte consecutive.	Numero di connessioni LoadBalancer rifiutate dall'appl icazione CloudWatch allarme se il numero di connessioni che sono state rifiutate perché il sistema di bilanciamento del carico ha raggiunto il suo massimo
Obiettivo Application Load Balancer	TargetConnectionErrorCount	$ {ElasticLoadBalancingV2:::T argetGroup:FullName} - Numero di errori di connessio

Tipo di servizio/risorsa	Fonte dell'avviso e condizione di attivazione	Nome e note dell'avviso
	(HTTPCode_target_5xx_count/ RequestCount) *100 somma > 15% per 1 minuto, 5 volte consecutive.	ne a Application LoadBalancer Target - $ {ElasticLoadBalancingV2:TargetGroup: :UUID} CloudWatch allarme relativo al numero eccessivo di codici di risposta HTTP 5XX generati da un target.
Obiettivo Application Load Balancer	ApplicationLoadBalancerTargetGroupErrorCount somma > 0% per 1 minuto, 5 volte consecutive.	$ {ElasticLoadBalancingV2:::TargetGroup:FullName} - Conteggio errori HTTP 5XX di Application LoadBalancer Target - $ {ElasticLoadBalancingV2:: TargetGroup :UUID} CloudWatch allarme se il numero di connessioni è stato stabilito senza successo tra il sistema di bilanciamento del carico e le istanze registrate.
Istanza Amazon EC2: tutte OSs	CPUUtilization* > 95% per 5 minuti, 6 volte consecutive, se l'istanza non risponde a un comando di polling Systems Manager.	$ {EC2::}: CPU troppo alta InstanceId CloudWatch allarme. L'elevato utilizzo della CPU è un indicatore di un cambiamento nello stato dell'applicazione, ad esempio deadlock, loop infiniti, attacchi dannosi e altre anomalie. Direct-Customer-AlertsSi tratta di allarmi.

Tipo di servizio/risorsa	Fonte dell'avviso e condizione di attivazione	Nome e note dell'avviso
Istanza Amazon EC2: tutte OSs	StatusCheckFailed > 0% per 5 minuti, 3 volte consecutive.	$ {EC2::InstanceId}: Controllo dello stato non riuscito CloudWatch allarme. Status Check Failed indica che un'istanza Amazon EC2 con l'ID specificato non ha superato uno o più dei suoi controlli di stato automatic i. Ciò significa che l'istanza presenta un problema che le impedisce di funzionare correttamente o di essere raggiungibile.
Istanza Amazon EC2 - Linux	Mem_used_percent minimo >= 95% per 5 minuti, 6 volte consecutive.	$ {EC2::InstanceId}: Senza memoria CloudWatch allarme. Memory Free indica che la memoria disponibile (RAM) sull'istanza Amazon EC2 specificata è scesa al di sotto di una soglia definita. Ciò può causare problemi di memoria, arresti anomali del sistema e indica che l'istanza potrebbe aver bisogno di più RAM. Questi sono Direct-Customer-Alerts allarmi.

Tipo di servizio/risorsa	Fonte dell'avviso e condizione di attivazione	Nome e note dell'avviso
Istanza Amazon EC2 - Linux	Swap_used_percent medio >= 95% per 5 minuti, 6 volte consecutive.	$ {EC2::InstanceId}: Swap gratuito CloudWatch allarme. Il valore medio di swap_used_percent su un'istanza Amazon EC2 indica che la percentuale media di spazio di swap allocato attualmente in uso ha superato una soglia predefini ta. Ciò può causare un peggioramento delle prestazio ni, colli di bottiglia e problemi di memoria. Si tratta di allarmi. Direct-Cu stomer-Alerts
Istanza Amazon EC2 - Linux	Percentuale massima di utilizzo del disco >= 95% per 5 minuti, 6 volte consecutive.	$ {EC2::InstanceId}: Utilizzo del disco troppo elevato - $ {EC2: :Disk: :UUID} CloudWatch allarme. Utilizzo del disco troppo elevato indica che l'utilizzo del disco su uno specifico Amazon EC2 o sul disco identificato si avvicina alla capacità. Ciò può portare a un peggioramento delle prestazioni, a errori delle applicazioni e all'instabilità del sistema. Questi sono allarmi Direct-Cu stomer-Alerts.

Tipo di servizio/risorsa	Fonte dell'avviso e condizione di attivazione	Nome e note dell'avviso
Istanza Amazon EC2 - Windows	Memoria minima% di byte impegnati in uso **>=** 95% per 5 minuti, 6 volte consecutive.	$ {EC2::InstanceId}: Senza memoria CloudWatch allarme. Memory Free indica che la memoria disponibile (RAM) sull'istanza Amazon EC2 specificata è scesa al di sotto di una soglia definita. Ciò può causare problemi di memoria, arresti anomali del sistema e indica che l'istanza potrebbe aver bisogno di più RAM. Questi sono Direct-Customer-Alerts allarmi.
Istanza Amazon EC2 - Windows	LogicalDisk % massima di spazio libero **<=** 5% per 5 minuti, 6 volte consecutive.	$ {EC2::InstanceId}: Utilizzo del disco troppo elevato - $ {EC2: :Disk: :UUID} CloudWatch allarme. Indica che la percentuale di spazio libero su un disco logico (una partizione del file system) all'interno di un'istanza Amazon EC2 Windows ha superato una soglia predefini ta. La carenza di spazio su disco può causare carenze di spazio su disco Si tratta di allarmi Direct-Cu stomer-Alerts.

Tipo di servizio/risorsa	Fonte dell'avviso e condizione di attivazione	Nome e note dell'avviso
Amazon EFS	AMSEFSBurstCreditBalanceExhausted. BurstCreditBalance meno di 1000 per quindici minuti.	$ {EFS::FileSystemId}: EFS: Burst Credit Balance CloudWatch allarme sul BurstCreditBalance file system Amazon EFS.
Amazon EFS	AMSEFSClientConnectionsLimit. ClientConnections > 24.000 per quindici minuti.	$ {EFS::FileSystemId}: EFS: Limite di connessioni client CloudWatch allarme sul ClientConnections file system Amazon EFS.
Amazon EFS	AMSEFSThroughputUtilizationLimit. Utilizzo del throughput EFS > 80% per un'ora.	$ {EFS::FileSystemId}: EFS: limite di utilizzo del throughput CloudWatch allarme sull'utilizzo del throughput del file system Amazon EFS.
Amazon EFS	AMSEFSPercentIOLimit. Percentuale IOLimit > 95 per settantacinque minuti.	$ {EFS::FileSystemId}: EFS: Percentuale IOLimit CloudWatch allarme sulla percentuale IOLimit del file system Amazon EFS.
Amazon EKS	Vedi Amazon EKSAvvisi di base per il monitoraggio e la gestione degli incidenti per Amazon EKS in AMS Accelerate.	

Tipo di servizio/risorsa	Fonte dell'avviso e condizione di attivazione	Nome e note dell'avviso
Istanza Elastic Load Balancing	SpilloverCountBack endConnectionErrors > 1 per 1 minuto, 15 volte consecutive.	Allarme LoadBalancer Spillover Count Classic CloudWatch allarme se un numero eccessivo di richieste sono state rifiutate perché la coda di sovratensione è piena.
Istanza Elastic Load Balancing	HTTPCode_ELB_5XX_Count somma > 0 per 5 minuti, 3 volte consecutive.	CloudWatch allarme relativo al numero eccessivo di codici di risposta HTTP 5XX che provengono dal load balancer.
Istanza Elastic Load Balancing	SurgeQueueLength > 100 per 1 minuto, 15 volte consecutive.	LoadBalancer Allarme Classic Surge Queue per la lunghezza della coda. CloudWatch allarme se un numero eccessivo di richieste è in attesa di instradamento.
FSx per ONTAP	AMSFSXONTAPIOPSUti lization. Utilizzo IOPS di FSX:ONTAP > 80% per due ore.	$ {FSx::}: Utilizzo di FSX:ONTAP IOPS FileSyste mId CloudWatch allarme sul limite di utilizzo IOPS dell'istanza for ONTAP. FSx
FSx per ONTAP	AMSFSXONTAPThrough putUtilizzo. Utilizzo del throughput di FSX:ONTAP > 80% per due ore.	$ {FSx::}: FSX:ONTAP Utilizzo del throughput FileSystemId CloudWatch allarme sul limite di throughput del volume for ONTAP. FSx

Tipo di servizio/risorsa	Fonte dell'avviso e condizione di attivazione	Nome e note dell'avviso
FSx per ONTAP	AMSFSXONTAPVolumeInodeUtilization. FSX:Utilizzo degli inodi ONTAP > 80% per due ore.	$ {FSx::} :$ {: :ONTAP::FileSystemId} Utilizzo degli inodi FSx FSX:ONTAP VolumeId CloudWatch allarme sul limite di utilizzo della capacità dei file del volume for ONTAP. FSx
FSx per ONTAP	AMSFSXONTAPVolumeCapacityUtilization. FSX:ONTAP Volume di utilizzo > 80% per due ore.	$ {FSx::} :$ {: FileSystemId :ONTAP::} FSx VolumeId CloudWatch allarme sul limite di utilizzo della capacità di volume del volume ONTAP. FSx
FSx per Windows File Server	AMSFSXWindowsThroughputUtilization. FSX:Utilizzo della velocità effettiva di Windows > 80% per due ore.	$ {FSx::}: FileSystemId FSX:Utilizzo della velocità effettiva di Windows CloudWatch allarme sul limite di velocità effettiva dell'istanza per Windows File Server. FSx
FSx per Windows File Server	AMSFSXWindowsIOPSUtilization. FSX:Utilizzo IOPS di Windows > 80% per due ore.	$ {FSx::}: FileSystemId FSX:Utilizzo IOPS di Windows CloudWatch allarme sul limite di utilizzo IOPS dell'istanza per Windows File Server. FSx

Tipo di servizio/risorsa	Fonte dell'avviso e condizione di attivazione	Nome e note dell'avviso
GuardDuty Servizio	Non applicabile; tutti i risultati (ai fini della minaccia) vengono monitorati. Ogni risultato corrisponde a un avviso. Modifiche nei GuardDuty risultati. Queste modifiche includono i nuovi risultati generati e le occorrenz e successive dei risultati esistenti.	Per un elenco dei tipi di GuardDuty ricerca supportat i, vedere GuardDuty Active Finding Types.
Integrità	Dashboard AWS Health	Le notifiche vengono inviate quando si verifican o cambiamenti nello stato di Dashboard AWS Health (AWS Health) eventi che richiedono l'intervento di AMS Operations in relazione ai servizi monitorati da AMS. Per ulteriori informazioni, consulta Servizi supportati.
IAM	Il profilo di istanza IAM di Amazon EC2 non esiste. Manca il profilo dell'istanza IAM.	Per istruzioni sulla sostituzi one di un profilo di istanza IAM di Amazon EC2, consulta la documentazione IAM nel ruolo Replace IAM.

Tipo di servizio/risorsa	Fonte dell'avviso e condizione di attivazione	Nome e note dell'avviso
IAM	Il profilo di istanza IAM di Amazon EC2 ha troppe policy. Il profilo dell'istanza IAM ha 10 policy e non è possibile aggiungere policy aggiuntive.	• Modifica la quota AWS di servizio per IAM per aumentare il numero di policy gestite per ruolo a 20. Per informazioni sulle quote di servizio, consulta Visualizzazione delle quote di servizio. • Riduci il numero di policy gestite al di sotto della quota IAM corrente rimuovendo le policy gestite non necessari e per il ruolo IAM associato a queste istanze. Assicurat i di mantenere le policy richieste da AMS. • Riduci il numero di policy gestite al di sotto dell'attu ale quota IAM consolida ndo le policy per il ruolo IAM associato a queste istanze. Assicurati di mantenere le policy richieste da AMS. Per le politiche richieste da AMS, consulta la Guida per l'utente di AMS Accelerat e:Dettagli della modifica delle autorizzazioni IAM.

Tipo di servizio/risorsa	Fonte dell'avviso e condizione di attivazione	Nome e note dell'avviso
Macie	Avvisi appena generati e aggiornamenti agli avvisi esistenti. Macie rileva eventuali modifiche nei risultati. Queste modifiche includono i nuovi risultati generati e le occorrenze successive dei risultati esistenti.	Avviso Amazon Macie. Per un elenco dei tipi di avviso Amazon Macie supportati, consulta Analisi dei risultati di Amazon Macie. Tieni presente che Macie non è abilitato per tutti gli account.
NATGateways	PacketsDropCount : Allarme se packetsdropcount è > 0 per un periodo di 15 minuti	NatGateway PacketsDr opCount Un valore superiore a zero potrebbe indicare un problema passeggero in corso con il gateway NAT.
NATGateways	ErrorPortAllocation : Allarme se i gateway NAT non sono riusciti ad allocare la porta per un periodo di valutazione superiore a 15 minuti	NatGateway ErrorPortAllocatio n Il numero di volte che il gateway NAT potrebbe non allocare una porta di origine. Un valore maggiore di zero indica che sono aperte troppe connessioni simultanee.

Tipo di servizio/risorsa	Fonte dell'avviso e condizione di attivazione	Nome e note dell'avviso
OpenSearch ammasso	ClusterStatus il massimo in rosso è >= 1 per 1 minuto, 1 volta consecutiva.	ClusterStatus Rosso CloudWatch allarme. La chiave di AWS KMS crittografia utilizzata per crittografare i dati inattivi nel dominio è disabilitata. Riabilitala per ripristinare le normali operazioni. Per ulteriori informazioni, consulta Red Cluster Status.
OpenSearch dominio	KMSKeyErrore >= 1 per 1 minuto, 1 volta consecutiva.	Errore chiave KMS CloudWatch allarme. Almeno una partizioni primaria e le relative repliche non sono assegnate a un nodo. Per ulteriori informazioni, consulta Encryption of Data at Rest for Amazon OpenSearch Service.
OpenSearch dominio	KMSKeyInaccessibile >= 1 per 1 minuto, 1 volta consecutiva.	Errore di inaccessibilità della chiave KMS CloudWatch allarme. Almeno una partizioni primaria e le relative repliche non sono assegnate a un nodo. Per ulteriori informazioni, consulta Encryption of Data at Rest for Amazon OpenSearch Service.

Tipo di servizio/risorsa	Fonte dell'avviso e condizione di attivazione	Nome e note dell'avviso
OpenSearch dominio	ClusterStatus il massimo giallo è >= 1 per 1 minuto, 1 volta consecutiva.	ClusterStatus Giallo Almeno una partizione di replica non è allocata per un nodo. Per ulteriori informazioni, consulta Yellow Cluster Status.
OpenSearch dominio	FreeStorageSpace il minimo è <= 20480 per 1 minuto, 1 volta consecutiva.	Spazio di archiviazione libero insufficiente Un nodo nel cluster è legato ai 20 GiB di spazio di archiviazione gratuito. Per ulteriori informazioni, vedi Mancanza di spazio di archiviazione disponibile.
OpenSearch dominio	ClusterIndexWritesBlocked >= 1 per 5 minuti, 1 volta consecutiva.	Cluster Index: scritture bloccate Il cluster sta bloccando le richieste di scrittura. Per ulteriori informazioni, consulta ClusterBlockException.
OpenSearch dominio	Nodi minimo < x per 1 giorno, 1 volta consecutiva.	Nodi inattivi x è il numero di nodi del cluster. Questo allarme indica che almeno un nodo nel cluster è stato irraggiungibile per un giorno. Per ulteriori informazioni, consulta Failed Cluster Nodes.

Tipo di servizio/risorsa	Fonte dell'avviso e condizione di attivazione	Nome e note dell'avviso
OpenSearch dominio	CPUUtilization media >= 80% per 15 minuti, 3 volte consecutive.	Utilizzo elevato della CPU nel nodo dati Il 100% di utilizzo della CPU non è raro, ma medie costantemente elevate sono problematiche. Valuta la possibilità di ridimensionare correttamente i tipi di istanze esistenti o di aggiungere istanze.
OpenSearch dominio	JVMMemoryPressione massimo >= 80% per 5 minuti, 3 volte consecutive.	Elevato utilizzo della memoria nel nodo dati Sui cluster potrebbero verificar si errori di esaurimento della memoria nel caso in cui l'utilizzo aumenti. Considera il dimensionamento verticale . OpenSearch impiega la metà della RAM di un'istanz a per l'heap Java, fino a una dimensione heap di 32 GiB. Puoi scalare le istanze verticalmente fino a 64 GiB di RAM e poi scalare orizzonta lmente aggiungendo le istanze.

Tipo di servizio/risorsa	Fonte dell'avviso e condizione di attivazione	Nome e note dell'avviso
OpenSearch dominio	Padrone CPUUtilization media >= 50% per 15 minuti, 3 volte consecutive.	Master Nodes: elevato utilizzo della CPU Prendi in considerazione l'utilizzo di tipi di istanze più grandi per i tuoi nodi master dedicati. A causa del loro ruolo nella stabilità del cluster e nelle distribuzioni blu/verde, i nodi master dedicati devono avere un utilizzo medio ridotto della CPU rispetto ai nodi di dati.
OpenSearch dominio	JVMMemoryPressione principale massimo >= 80% per 15 minuti, 1 volta consecutiva.	Master Nodes: elevata pressione della memoria JVM Prendi in considerazione l'utilizzo di tipi di istanze più grandi per i tuoi nodi master dedicati. A causa del loro ruolo nella stabilità del cluster e nelle distribuzioni blu/verde, i nodi master dedicati devono avere un utilizzo medio ridotto della CPU rispetto ai nodi di dati.

Tipo di servizio/risorsa	Fonte dell'avviso e condizione di attivazione	Nome e note dell'avviso
OpenSearch istanza	AutomatedSnapshotFailure il massimo è >= 1 per 1 minuto, 1 volta consecutiva.	Errore automatico della copia istantanea CloudWatch allarme. Uno snapshot automatico ha restituito un errore. Questo errore è spesso il risultato di uno stato del cluster rosso. Per saperne di più, consulta Red Cluster Status.
Amazon RDS	Utilizzo medio della CPU > 90% per 15 minuti, 2 volte consecutive.	$ {RDS:: DBInstance Identificatore}: CPUUtilization CloudWatch allarmi.
Amazon RDS	Somma di DiskQueueDepth > 75% per 1 minuto, 15 volte consecutive.	$ {RDS:: DBInstance Identificatore}: DiskQueue CloudWatch allarmi.
Amazon RDS	Media FreeStorageSpace < 1.073.741.824 byte per 5 minuti, 2 volte consecutive.	$ {RDS:: Identificatore}: DBInstance FreeStorageSpace CloudWatch allarmi.
Amazon RDS	Avviso di archiviazione insufficiente Si attiva quando lo storage allocato per l'istanza DB è esaurito.	RDS-EVENT-0007, consulta i dettagli in Utilizzo della notifica degli eventi di Amazon RDS.

Tipo di servizio/risorsa	Fonte dell'avviso e condizione di attivazione	Nome e note dell'avviso
Amazon RDS	Errore dell'istanza DB L'istanza database ha avuto esito negativo a causa di una configurazione non compatibile o di un problema di storage sottostante. Inizia a point-in-time-restore per l'istanza DB.	RDS-EVENT-0031, consulta i dettagli in Categorie di eventi e messaggi di eventi di Amazon RDS.
Amazon RDS	Il failover RDS -0034 non è stato tentato. Amazon RDS non sta tentando di effettuare un failover richiesto perché di recente si è verificato un failover nell'istanza database.	RDS-EVENT-0034, consulta i dettagli in Categorie di eventi e messaggi di eventi di Amazon RDS.
Amazon RDS	RDS - Parametri non validi dell'istanza DB 0035 Ad esempio, MySQL non può avviarsi perché un parametro relativo alla memoria è impostato su un valore troppo alto per questa classe di istanze, quindi l'azione da eseguire sarebbe modificare il parametro di memoria e riavviare l'istanza DB.	RDS-EVENT-0035, consulta i dettagli in Categorie di eventi e messaggi di eventi di Amazon RDS.

Tipo di servizio/risorsa	Fonte dell'avviso e condizione di attivazione	Nome e note dell'avviso
Amazon RDS	Istanza DB di sottorete non valida IDs L'istanza database si trova in una rete non compatibile. Alcune delle sottoreti specifica te non IDs sono valide o non esistono.	Evento di servizio. RDS-EVENT-0036, consulta i dettagli in Categorie di eventi e messaggi di eventi di Amazon RDS.
Amazon RDS	Errore di lettura della replica dell'istanza DB RDS-0045 Si è verificato un errore interno nel processo di replica di lettura. Per ulteriori informazi oni, consulta il messaggio di evento. Per informazioni sulla risoluzione degli errori di Read Replica, consulta Risoluzio ne di un problema di Read Replica di MySQL.	RDS-EVENT-0045, consulta i dettagli in Categorie di eventi e messaggi di eventi di Amazon RDS.
Amazon RDS	RDS-0057 Errore durante la creazione dell'account utente statspack La replica su Read Replica è stata terminata.	Evento di servizio. RDS-EVENT-0057, consulta i dettagli in Categorie di eventi e messaggi di eventi di Amazon RDS.

Tipo di servizio/risorsa	Fonte dell'avviso e condizione di attivazione	Nome e note dell'avviso
Amazon RDS	La replica di lettura dell'istanza DB RDS-0058 è terminata Errore durante la creazione dell'account utente Statspack PERFSTAT. Elimina l'account prima di aggiungere l'opzione Statspack.	Evento di servizio. RDS-EVENT-0058, consulta i dettagli in Categorie di eventi e messaggi di eventi di Amazon RDS.
Amazon RDS	Avvio del ripristino dell'istanza DB L'istanza database di SQL Server sta ristabilendo il relativo mirror. Le prestazioni subiranno un peggioramento fino al termine dell'operazione. È stato trovato un database con un modello di recupero non FULL. Il modello di ripristino è stato riportato a FULL ed è stato avviato il ripristino in mirroring. (<dbname>: <recovery model found>[,...])	Evento di servizio. RDS-EVENT-0066, consulta i dettagli nelle categorie di eventi e messaggi di eventi di Amazon RDS.
Amazon RDS	Il failover del cluster di database non è riuscito.	RDS-EVENT-0069, consulta i dettagli in Categorie di eventi e messaggi di eventi di Amazon RDS.

Tipo di servizio/risorsa	Fonte dell'avviso e condizione di attivazione	Nome e note dell'avviso
Amazon RDS	Bucket S3 di ripristino delle autorizzazioni non valide Il ruolo IAM utilizzato per accedere al bucket di Amazon S3 per il backup e ripristino nativo di SQL Server non è configurato correttamente. Per ulteriori informazioni, vedere Configurazione per il backup e il ripristino nativi.	Evento di servizio. RDS-EVENT-0081, consulta i dettagli nelle categorie di eventi e messaggi di eventi di Amazon RDS.
Amazon RDS	Aurora non è riuscito a copiare i dati di backup da un bucket Simple Storage Service (Amazon S3).	RDS-EVENT-0082, consulta i dettagli in Categorie di eventi e messaggi di eventi di Amazon RDS.
Amazon RDS	Avviso di storage insuffici ente quando l'istanza DB ha consumato più del 90% dello storage allocato.	Evento di servizio. RDS-EVENT-0089, consulta i dettagli nelle categorie di eventi e messaggi di eventi di Amazon RDS.
Amazon RDS	Il servizio di notifica durante il ridimensionamento non è riuscito per il cluster DB Aurora Serverless.	Evento di servizio. RDS-EVENT-0143, consulta i dettagli in Categorie di eventi e messaggi di eventi di Amazon RDS.
Amazon RDS	L'istanza database è in uno stato non valido. Nessuna operazione richiesta. Il ridimensionamento automatico verrà riprovato in un secondo momento.	RDS-EVENT-0219, consulta i dettagli in Categorie di eventi e messaggi di eventi di Amazon RDS.

Tipo di servizio/risorsa	Fonte dell'avviso e condizione di attivazione	Nome e note dell'avviso
Amazon RDS	L'istanza database ha raggiunto la soglia completa dello storage e il database è stato arrestato.	RDS-EVENT-0221, consulta i dettagli in Categorie di eventi e messaggi di eventi di Amazon RDS.
Amazon RDS	Questo evento indica che la scalabilità automatica dello storage delle istanze di Amazon RDS non è in grado di scalare, i motivi per cui l'autoscaling non è riuscito possono essere diversi.	RDS-EVENT-0223, consulta i dettagli in Categorie di eventi e messaggi di eventi di Amazon RDS.
Amazon RDS	La scalabilità automatica dello storage ha attivato un'attivi tà di storage in sospeso che avrebbe raggiunto la soglia massima di storage.	RDS-EVENT-0224, consulta i dettagli in Categorie di eventi e messaggi di eventi di Amazon RDS.
Amazon RDS	Il tipo di archiviazione dell'ista nza database non è attualmen te disponibile nella zona di disponibilità. Il ridimensi onamento automatico verrà riprovato in un secondo momento.	RDS-EVENT-0237, consulta i dettagli in Categorie di eventi e messaggi di eventi di Amazon RDS.
Amazon RDS	Amazon RDS non è riuscito a fornire capacità per il proxy perché non ci sono abbastanz a indirizzi IP disponibili nelle tue sottoreti.	RDS-EVENT-0243, consulta i dettagli in Categorie di eventi e messaggi di eventi di Amazon RDS.

Tipo di servizio/risorsa	Fonte dell'avviso e condizione di attivazione	Nome e note dell'avviso
Amazon RDS	Lo spazio di archiviazione del tuo Account AWS ha superato la quota di spazio di archiviazione consentita.	RDS-EVENT-0254, consulta i dettagli in Categorie di eventi e messaggi di eventi di Amazon RDS.
Cluster Amazon Redshift	Lo stato del cluster quando non è in modalità di manutenzione < 1 per 5 minuti	RedshiftClusterHealthStatus Per ulteriori informazioni, consulta Monitoraggio di Amazon Redshift tramite CloudWatch metriche.
Site-to-Site VPN	VPNTunnelGiù TunnelState <= 0 per 1 minuto, 20 volte consecutive.	$ {AWS::EC2::VpnConnectionId} - Giù VPNTunnel TunnelState è 0 quando entrambi i tunnel sono inattivi, .5 quando un tunnel è attivo e 1,0 quando entrambi i tunnel sono attivi.
Agente Systems Manager	Istanze EC2 non gestite da Systems Manager L'agente SSM non è installato. L'agente SSM è installato sull'istanza, ma il servizio dell'agente non è in esecuzione. L'agente SSM non dispone di un percorso di rete verso il servizio AWS Systems Manager.	Esistono condizioni aggiuntive che causano l'interruzione del Systems Manager Agent; per ulteriori informazioni, vedere Risoluzione dei problemi relativi alla disponibilità dei nodi gestiti.

Per informazioni sulle azioni correttive, consulta. Correzione automatica degli avvisi con AMS

Guardate il video di Andrew per saperne di più (7:03)

Notifiche di incidenti con riconoscimento delle applicazioni in AMS

Utilizza le notifiche automatiche di incidenti basate sull'applicazione per personalizzare la tua esperienza di comunicazione per i casi di supporto creati da AMS per tuo conto. Quando utilizzi questa funzione, AMS recupera le preferenze personalizzate relative ai carichi di lavoro AWS Service Catalog AppRegistryper arricchire le comunicazioni relative agli incidenti AMS con metadati sulle tue applicazioni e personalizzare la gravità dei casi di supporto creati da AMS per tuo conto. Per utilizzare questa funzionalità, devi prima effettuare l'onboarding di. AWS Service Catalog AppRegistry

Per ulteriori informazioni sui valori predefiniti di monitoraggio di AMS Accelerate, consulta. Monitoraggio e gestione degli eventi in AMS Accelerate

Accedi AppRegistry e crea applicazioni

Per effettuare l'onboarding AppRegistry, consulta Getting started with AppRegistry nella AWS Service Catalog AppRegistry Administrator Guide. Dopo l'onboarding, utilizza uno dei seguenti metodi per creare applicazioni:

1. AWS console: per ulteriori informazioni sulla creazione di un'applicazione AppRegistry tramite la AWS console, consulta Creazione di applicazioni nella Guida per l'AWS Service Catalog AppRegistry amministratore.
2. CloudFormation: È possibile definire AppRegistry l'applicazione proprio come si definisce qualsiasi altra risorsa. Per ulteriori informazioni, consulta Riferimento al tipo di risorsa AWS Service Catalog AppRegistry nella Guida dell'utente di CloudFormation .
3. Automazione AMS: per semplificare il processo di registrazione dell'applicazione, AMS fornisce il documento `AWSManagedServices-CreateAppRegistryApplication` di automazione SSM. Per utilizzare questo metodo, richiamate il documento dalla AWS Systems Manager console all'indirizzo https://console.aws.amazon.com/systems-manager/o con il AWS CLI come descritto nell'esempio seguente.

```
# The following registers a new application with customized severity
aws ssm start-automation-execution \
  --document-name "AWSManagedServices-CreateAppRegistryApplication" \
  --parameters '{"ResourceAssociationType":["TAGS"],"AppTagValue":
["MyApp"],"CFNStackNames":[],"ApplicationName":
["BananaStand"],"ApplicationDescription":["This is my banana stand
```

```
 application"],"AppCriticality":["normal"],"AutomationAssumeRole":
["arn:aws:iam::123456789012:role/SSMAdminRole"]}' \
  --region us-east-1
# The following registers a new application with no customizations
aws ssm start-automation-execution \
  --document-name "AWSManagedServices-CreateAppRegistryApplication" \
  --parameters '{"ResourceAssociationType":["TAGS"],"AppTagValue":
["MyApp"],"CFNStackNames":[],"ApplicationName":
["BananaStand"],"ApplicationDescription":["This is my banana stand
 application"],"AppCriticality":["unset"],"AutomationAssumeRole":
["arn:aws:iam::123456789012:role/SSMAdminRole"]}' \
  --region us-east-1
# You can also register applications using CloudFormation stacks
aws ssm start-automation-execution \
  --document-name "AWSManagedServices-CreateAppRegistryApplication" \
  --parameters '{"ResourceAssociationType":["STACKS"],"AppTagValue":
[""],"CFNStackNames":["arn:aws:cloudformation:us-east-1:123456789012:stack/
stack-2343eddq/1a2b3c4d-5e6f-7g8h-9i0j-1k2l3m4n5o6p"],"ApplicationName":
["BananaStand"],"ApplicationDescription":["This is my banana stand
 application"],"AppCriticality":["unset"],"AutomationAssumeRole":
["arn:aws:iam::123456789012:role/SSMAdminRole"]}' \
  --region us-east-1
```

Crea tag per abilitare l'arricchimento dei casi

È necessario etichettare le applicazioni prima che AMS possa accedere ai metadati delle applicazioni. La tabella seguente elenca i tag richiesti.

I tag con il prefisso `ams:rt:` vengono applicati tramite Resource Tagger.

Chiave tag	Valore tag
è gestito da ams	true
ams:rt:ams-managed	true

Personalizza la gravità dei casi di supporto AMS per le tue applicazioni

Puoi personalizzare la gravità dei casi di supporto creati da AMS specificando l'importanza dell'applicazione per l'organizzazione. Questa impostazione è controllata da un gruppo di attributi

associato all'applicazione in AppRegistry. Il nome del nome del gruppo di attributi deve corrispondere al seguente schema:

```
AMS.<ApplicationName>.CommunicationOptions
```

Nello schema precedente, `ApplicationName` deve corrispondere al nome utilizzato al AppRegistry momento della creazione dell'applicazione.

Contenuto di esempio:

```
{
"SchemaVersion": "1.0",
"Criticality": "low"
}
```

SchemaVersion

Ciò determina la versione dello schema che stai utilizzando e il sottoinsieme di funzionalità disponibili per l'uso.

Versione dello schema	Funzionalità
1.0	Severità personalizzata dei casi di supporto in base al valore di criticità

Criticità

La criticità di questa applicazione determina la gravità dei casi di supporto creati dai sistemi automatizzati AMS.

Valori validi:

```
low|normal|high|urgent|critical
```

Per ulteriori informazioni sui livelli di gravità, consulta SeverityLevelI'Supporto AWS API Reference.

Campo obbligatorio: sì

Rivedi le autorizzazioni richieste

Per utilizzare questa funzionalità, AMS richiede l'accesso alle seguenti autorizzazioni: AWS Identity and Access Management

- Io sono: ListRoleTags
- Io sono: ListUserTags
- sourcegrouptaggingapi: GetResources
- service catalog-app: GetApplication
- servicecatalog-app: ListAssociatedAttributeGroups
- servicecatalog-app: GetAttributeGroup

> **Important**
>
> Assicurati che non esista una policy IAM o una policy di controllo del servizio (SCP) che neghi le azioni precedenti.

Le chiamate API vengono effettuate dal ruolo. `ams-access-admin` Di seguito è riportato un esempio di ciò che potresti vedere:

```
arn:aws:sts::111122223333:assumed-role/ams-access-admin/AMS-AMSAppMetadataLookup-*
```

Accelera Alarm Manager

AMS Accelerate applica allarmi alle tue AWS risorse utilizzando Alarm Manager basato su tag per implementare una strategia di monitoraggio di base e garantire che tutte le tue AWS risorse siano monitorate e protette. Grazie all'integrazione con Alarm Manager basato su tag, è possibile personalizzare la configurazione delle AWS risorse in base al tipo, alla piattaforma e ad altri tag, per garantire il monitoraggio delle risorse. Alarm Manager viene distribuito sull'account Accelerate durante l'onboarding.

Come funziona Alarm Manager

Quando l'account viene registrato su AMS Accelerate, nell'account vengono distribuiti due documenti JSON, chiamati profili di configurazione, in. AWS AppConfig Entrambi i documenti di profilo risiedono nell'applicazione Alarm Manager e nell'ambiente dell'infrastruttura AMS Accelerate.

I due profili di configurazione sono denominati AMSManagedAlarms (il profilo di configurazione predefinito) e CustomerManagedAlarms(il profilo di configurazione di personalizzazione).

- Profilo di configurazione predefinito:
  - La configurazione trovata in questo profilo contiene la configurazione predefinita che AMS Accelerate implementa in tutti gli account dei clienti. Questa configurazione contiene la politica di monitoraggio predefinita di AMS Accelerate.

    > **Important**
    >
    > Non modificate questo profilo perché AMS Accelerate può aggiornarlo in qualsiasi momento, cancellando le modifiche apportate.

  - Se desideri modificare o disabilitare una di queste definizioni, consulta Modifica della configurazione predefinita di Accelerate alarm eDisattivazione della configurazione predefinita di Accelerate alarm.
- Profilo di configurazione di personalizzazione:
  - Qualsiasi configurazione in questo profilo è gestita interamente dall'utente; AMS Accelerate non sovrascrive questo profilo, a meno che l'utente non lo richieda esplicitamente.
  - Puoi specificare tutte le definizioni di allarme personalizzate che desideri in questo profilo e puoi anche specificare modifiche alla configurazione predefinita gestita da AMS Accelerate. Per ulteriori informazioni, consultare Modifica della configurazione predefinita di Accelerate alarm e Disattivazione della configurazione predefinita di Accelerate alarm.
  - Se aggiorni questo profilo, Alarm Manager applica automaticamente le modifiche a tutte le risorse pertinenti del tuo account. AWS
  - Puoi aggiornare questo profilo utilizzando gli CLI/SDK strumenti Console di gestione AWS o AWS. Consulta la Guida per AWS AppConfig l'utente per istruzioni sull'aggiornamento di una configurazione.
  - Il profilo di personalizzazione è inizialmente vuoto; tuttavia, tutte le definizioni di allarme inserite nel documento del profilo vengono applicate, oltre alla configurazione predefinita.

Tutti gli CloudWatch allarmi creati da Alarm Manager contengono la chiave di tag ams:alarm-manager:managed e tag value true. Questo serve a garantire che Alarm Manager gestisca solo gli allarmi che crea e non interferisca con nessuno dei tuoi allarmi. Puoi visualizzare questi tag utilizzando l' CloudWatch ListTagsForResourceAPI Amazon.

> **Important**
>
> Se le definizioni di allarme personalizzate e le definizioni di allarme predefinite vengono specificate con lo stesso ConfigurationID (vediAccelera il profilo di configurazione: monitoraggio), le definizioni personalizzate hanno la priorità sulle regole predefinite.

Guida introduttiva ad Accelerate Alarm Manager

Per impostazione predefinita, quando si effettua l'onboarding con AMS Accelerate, la configurazione viene implementata su AWS AppConfig, definendo una linea di base di allarme per le risorse. Le definizioni degli allarmi vengono applicate solo alle risorse con i tag ams:rt: *. Si consiglia di applicare questi tag utilizzandoAccelera Resource Tagger: si imposta una configurazione di base di Resource Tagger per far sapere ad AMS Accelerate quali risorse si desidera gestire.

Usa Resource Tagger per applicare la chiave di tag ams:rt:ams-managed con il valore del tag true a tutte le risorse che desideri che AMS Accelerate controlli.

Di seguito è riportato un esempio di profilo di personalizzazione di Resource Tagger che puoi utilizzare per attivare il monitoraggio di tutte le tue istanze Amazon EC2 . Per informazioni generali, vedi Accelera Resource Tagger.

```
{
    "AWS::EC2::Instance": {
        "AMSManageAllEC2Instances": {
            "Enabled": true,
            "Filter": {
                "InstanceId": "*"
            },
            "Tags": [
                {
                    "Key": "ams:rt:ams-managed",
                    "Value": "true"
                }
            ]
```

```
        }
    }
}
```

Per informazioni su come applicare questa configurazione di Resource Tagger, consulta. Visualizzazione o modifica della configurazione di Resource Tagger

Accelera i tag di Alarm Manager

Per impostazione predefinita, quando si effettua l'onboarding con AMS Accelerate, la configurazione viene implementata per AWS AppConfig definire una base di allarme per le risorse. Le definizioni degli allarmi vengono applicate solo alle risorse con i tag ams:rt: *. Si consiglia di applicare questi tag utilizzandoAccelera Resource Tagger: si imposta una configurazione di base di Resource Tagger per far sapere ad AMS Accelerate quali risorse si desidera gestire.

Usa Resource Tagger per applicare la chiave di tag ams:rt:ams-managed con il valore del tag true a tutte le risorse che desideri che AMS Accelerate controlli.

Argomenti

- Accelera i tag utilizzando Resource Tagger
- Accelera i tag senza Resource Tagger
- Accelera i tag utilizzando CloudFormation
- Accelera i tag usando Terraform

Accelera i tag utilizzando Resource Tagger

L'Alarm Manager basato su tag gestisce il ciclo di vita degli CloudWatch allarmi per risorsa; tuttavia, richiede che le risorse gestite abbiano tag specifici definiti da AMS Accelerate. Per utilizzare Resource Tagger per applicare il set predefinito di allarmi gestiti da AMS a istanze basate su Linux e Windows, segui questi passaggi.

1. Accedi alla console all'interno del tuo account. AppConfig
2. Seleziona l' ResourceTagger applicazione.
3. Seleziona la scheda Profili di configurazione, quindi seleziona CustomerManagedTags.
4. Fate clic su Crea per creare un nuovo profilo.
5. Seleziona JSON e definisci la tua configurazione. Per altri esempi di definizione di filtri e piattaforme, consultaAccelera Resource Tagger.

```
{
"AWS::EC2::Instance": {
   "MonitorAllInstances": {
       "Enabled": true,
       "Filter": {
           "Platform": "*"
       },
       "Tags": [
           {
               "Key": "ams:rt:ams-managed",
               "Value": "true"
           }
       ]
   }
}
}
```

6. Fai clic su Crea versione di configurazione ospitata.
7. Fai clic su Avvia distribuzione.
8. Definisci i seguenti dettagli di distribuzione:

```
Environment: AMSInfrastructure Hosted configuration version: <Select the version
 that you have just created>
              Deployment Strategy: AMSNoBakeDeployment
```

9. Fai clic su Avvia distribuzione.

Le istanze `"ams:rt:ams-monitoring-policy-platform": "ams-monitored-linux"` vengono etichettate con`"ams:rt:ams-managed": "true"`, il che garantisce l'applicazione `"ams:rt:ams-monitoring-policy": "ams-monitored"` di dati aggiuntivi alle istanze. Questi tag determinano quindi la creazione degli allarmi appropriati per l'istanza. Per ulteriori informazioni su questo processo, consulta Monitoraggio in Accelere.

Guardate il video di Himanshu per saperne di più (11:04)

Accelera i tag senza Resource Tagger

L'Alarm Manager basato su tag gestisce il ciclo di vita degli CloudWatch allarmi per risorsa; tuttavia, richiede che le risorse gestite abbiano tag specifici definiti da AMS Accelerate. AMS Accelerate

fornisce un profilo di configurazione predefinito che presuppone che i tag siano stati applicati da Resource Tagger.

Se desideri utilizzare un metodo alternativo per applicare tag alle tue risorse, come CloudFormation o Terraform e non Resource Tagger, devi disabilitare Resource Tagger in modo che non applichi tag alle tue risorse e competa con il metodo di tagging scelto. Per istruzioni su come modificare il profilo di configurazione personalizzato di Resource Tagger per abilitare la modalità di sola lettura, consulta. Impedire a Resource Tagger di modificare le risorse

Dopo aver impostato il Resource Tagger in modalità di sola lettura e aver distribuito il profilo di configurazione, utilizza il metodo di tagging scelto per applicare i tag alle risorse in base alle seguenti linee guida:

Tipo di risorsa	Chiave tag	Valore tag
Tutte le risorse supportate (descritte in questa tabella)	ams: rt: ams-monitoring-policy	sono monitorati
EC2 istanze (Linux)	ams: rt: ams-monitoring-policy-platform	ams-monitored-linux
EC2 istanze (Windows)	ams: rt: ams-monitoring-policy-platform	ams-monitored-windows
OpenSearch Dominio con KMS	ams: rt: ams-monitoring-with-kms	ams-monitored-with-kms
OpenSearch Dominio con nodo master dedicato	ams: rt: ams-monitoring-with-master	ams-monitored-with-master

Le risorse che hanno questi tag, chiavi e valori sono gestite da AMS Accelerate Alarm Manager.

Accelera i tag utilizzando CloudFormation

> **Note**
>
> Assicurati di aver impostato Resource Tagger in modalità di sola lettura prima di applicare i tag utilizzando CloudFormation, altrimenti Resource Tagger potrebbe modificare i tag in base

al profilo di configurazione. Per informazioni sull'impostazione di Resource Tagger in modalità di sola lettura e linee guida su come fornire tag personalizzati, consulta. Accelera i tag senza Resource Tagger

Per applicare i tag utilizzando CloudFormation, puoi applicare i tag a livello di stack (vedi Tag CloudFormation delle risorse) o, a livello di singola risorsa, (ad esempio, vedi Creazione EC2 di tag di istanza).

Di seguito è riportato un esempio di come è possibile applicare i tag di gestione degli allarmi di AMS Accelerate a un' EC2istanza Amazon gestita da CloudFormation:

```
Type: AWS::EC2::Instance
Properties:
 InstanceType: "t3.micro"

 # ...other properties...

 Tags:
   - Key: "aws:rt:ams-monitoring-policy"
     Value: "ams-monitored"
   - Key: "aws:rt:ams-monitoring-policy-platform"
     Value: "ams-monitored-linux"
```

Di seguito è riportato un esempio di come è possibile applicare i tag di gestione degli allarmi di AMS Accelerate a un gruppo Auto Scaling gestito da. CloudFormation Tieni presente che il gruppo Auto Scaling propagherà i propri tag alle EC2 istanze Amazon da esso create:

```
Type: AWS::AutoScaling::AutoScalingGroup
Properties:
 AutoScalingGroupName: "TestASG"

 # ...other properties...

 Tags:
   - Key: "aws:rt:ams-monitoring-policy"
     Value: "ams-monitored"
   - Key: "aws:rt:ams-monitoring-policy-platform"
     Value: "ams-monitored-linux"
```

Accelera i tag usando Terraform

> **Note**
>
> Assicurati di aver impostato Resource Tagger in modalità di sola lettura prima di applicare i tag utilizzando CloudFormation, altrimenti Resource Tagger potrebbe modificare i tag in base al profilo di configurazione. Per informazioni sull'impostazione di Resource Tagger in modalità di sola lettura e linee guida su come fornire tag personalizzati, consulta. Accelera i tag senza Resource Tagger

Per una descrizione di come gestire i tag delle risorse utilizzando Terraform, consulta la documentazione di Terraform Resource Tagging.

Di seguito è riportato un esempio di come è possibile applicare i tag di gestione degli allarmi AMS Accelerate a un' EC2istanza Amazon gestita da Terraform.

```
resource "aws_instance" "test_linux_instance" {
     # ...ami and other properties...

     instance_type = "t3.micro"

     tags = {
       "aws:rt:ams-monitoring-policy" = "ams-monitored"
       "aws:rt:ams-monitoring-policy-platform" = "ams-monitored-linux"
     }
   }
```

Di seguito è riportato un esempio di come è possibile applicare i tag di gestione degli allarmi AMS a un gruppo Auto Scaling gestito da Terraform. Nota che il gruppo Auto Scaling propaga i suoi tag alle EC2 istanze da esso create:

```
resource "aws_autoscaling_group" "test_asg" {
name = "terraform-test"
# ...other properties...

tags = {
  "aws:rt:ams-monitoring-policy" = "ams-monitored"
  "aws:rt:ams-monitoring-policy-platform" = "ams-monitored-linux"
```

```
 }
}
```

Accelera i profili di configurazione di Alarm Manager

Quando il tuo account viene registrato su AMS Accelerate, nell'account vengono distribuiti due documenti JSON, chiamati profili di configurazione, con AWS AppConfig (vedi Cos'è). AWS AppConfig Entrambi i documenti di profilo risiedono nell'applicazione Alarm Manager e nell'ambiente dell'infrastruttura AMS Accelerate.

Argomenti

- Accelera il profilo di configurazione: monitoraggio
- Accelera il profilo di configurazione: sostituzione di pseudoparametri
- Esempi di configurazione degli allarmi di accelerazione
- Visualizzazione della configurazione di Accelerate Alarm Manager
- Modifica della configurazione dell'allarme Accelerate
- Modifica della configurazione predefinita di Accelerate alarm
- Implementazione delle modifiche alla configurazione di Accelerate
- Rolling back Accelera le modifiche agli allarmi
- Mantenimento degli allarmi Accelerate
- Disattivazione della configurazione predefinita di Accelerate alarm

Accelera il profilo di configurazione: monitoraggio

Sia il documento del profilo di configurazione predefinito che il documento del profilo di configurazione di personalizzazione seguono la stessa struttura:

```
{
  "<ResourceType>": {
      "<ConfigurationID>": {
          "Enabled": true,

          "Tag": {
              "Key": "...",
              "Value": "..."
```

```
            },
            "AlarmDefinition": {
                ...
            }
        },
        "<ConfigurationID>": {
            ...
        }
    },
    "<ResourceType>": {
        ...
    }
}
```

- ResourceType: Questa chiave deve essere una delle seguenti stringhe supportate. La configurazione all'interno di questo oggetto JSON riguarderà solo il tipo di AWS risorsa specificato. Tipi di risorsa supportati:

```
AWS::EC2::Instance
AWS::EC2::Instance::Disk
AWS::RDS::DBInstance
AWS::Elasticsearch::Domain
AWS::OpenSearch::Domain
AWS::Redshift::Cluster
AWS::ElasticLoadBalancingV2::LoadBalancer
AWS::ElasticLoadBalancingV2::LoadBalancer::TargetGroup
AWS::ElasticLoadBalancing::LoadBalancer
AWS::FSx::FileSystem::ONTAP
AWS::FSx::FileSystem::ONTAP::Volume
AWS::FSx::FileSystem::Windows
AWS::EFS::FileSystem
AWS::EC2::NatGateway
AWS::EC2::VPNConnection
```

- ConfigurationID: questa chiave deve essere univoca nel profilo e denominare in modo univoco il seguente blocco di configurazione. Se si specifica un ConfigurationID nel profilo di personalizzazione uguale a quello specificato nel profilo predefinito, il blocco di configurazione definito nel profilo di personalizzazione ha effetto.
  - Abilitato: (opzionale, default=true) Specificate se il blocco di configurazione avrà effetto. Imposta questo valore su false per disabilitare un blocco di configurazione. Un blocco di configurazione disabilitato si comporta come se non fosse presente nel profilo.

- Tag: specifica il tag a cui si applica questa definizione di allarme. Qualsiasi risorsa (del tipo di risorsa appropriato) che abbia questa chiave e questo valore di tag avrà un CloudWatch allarme creato con la definizione data. Questo campo è un oggetto JSON con i seguenti campi:
  - Chiave: la chiave del tag da abbinare. Tieni presente che se utilizzi Resource Tagger per applicare i tag alla risorsa, la chiave per il tag inizierà sempre con ams:rt:.
  - Valore: il valore del tag da abbinare.
- AlarmDefinition: Definisce l'allarme da creare. Si tratta di un oggetto JSON i cui campi vengono passati così come sono alla chiamata CloudWatch `PutMetricAlarm` API (ad eccezione degli pseudoparametri; per ulteriori informazioni, vedere). Accelera il profilo di configurazione: sostituzione di pseudoparametri Per informazioni sui campi obbligatori, consultate la documentazione. PutMetricAlarm

  O

  CompositeAlarmDefinition: Definisce un allarme composito da creare. Quando si crea un allarme composito, si specifica un'espressione di regola per l'allarme che tiene conto dello stato di allarme di altri allarmi che hai creato. Si tratta di un oggetto JSON i cui campi vengono passati così come sono a. `CloudWatchPutCompositeAlarm` L'allarme composito entra in stato ALARM solo se tutte le condizioni della regola sono soddisfatte. Gli allarmi specificati nell'espressione di regola di un allarme composito possono includere allarmi di parametri e altri allarmi compositi. Per informazioni sui campi obbligatori, consultate la documentazione. PutCompositeAlarm

  Entrambe le opzioni forniscono i seguenti campi:

  - AlarmName: Specificate il nome dell'allarme che desiderate creare per la risorsa. Questo campo ha tutte le stesse regole specificate nella PutMetricAlarmdocumentazione; tuttavia, poiché il nome dell'allarme deve essere unico in una regione, Alarm Manager ha un requisito aggiuntivo: è necessario specificare lo pseudoparametro identificativo univoco nel nome dell'allarme (altrimenti, Alarm Manager aggiunge l'identificatore univoco della risorsa davanti al nome dell'allarme). Ad esempio, per il tipo di AWS::EC2::Instancerisorsa, è necessario specificare `${EC2::InstanceId}` il nome dell'avviso oppure viene aggiunto implicitamente all'inizio del nome dell'avviso. Per l'elenco degli identificatori, vedere. Accelera il profilo di configurazione: sostituzione di pseudoparametri

    Tutti gli altri campi sono quelli specificati nella PutMetricAlarmo nella PutCompositeAlarmdocumentazione.

- AlarmRule: Specificate quali altri allarmi devono essere valutati per determinare lo stato di questo allarme composito. Per ogni allarme a cui fai riferimento, devono essere presenti CloudWatch o specificati nel profilo di configurazione di Alarm Manager del tuo account.

> **Important**
>
> È possibile specificare uno dei due AlarmDefinitiono CompositeAlarmDefinitionnel documento di configurazione di Alarm Manager, ma entrambi non possono essere utilizzati contemporaneamente.

Nell'esempio seguente, il sistema crea un allarme quando due allarmi metrici specificati superano la soglia:

```
{
  "AWS::EC2::Instance": {
    "LinuxResourceAlarm": {
      "Enabled": true,
      "Tag": {
        "Key": "ams:rt:mylinuxinstance",
        "Value": "true"
      },
      "CompositeAlarmDefinition": {
        "AlarmName": "${EC2::InstanceId} Resource Usage High",
        "AlarmDescription": "Alarm when a linux EC2 instance is using too much CPU and
 too much Disk",
        "AlarmRule": "ALARM(\"${EC2::InstanceId}: Disk Usage Too High -
 ${EC2::Disk::UUID}\") AND ALARM(\"${EC2::InstanceId}: CPU Too High\")"
      }
    }
  }
}
```

> **Important**
>
> Quando Alarm Manager non è in grado di creare o eliminare un allarme a causa di un'interruzione della configurazione, invia la notifica all'argomento SNS Direct-Customer-Alerts. Questo AlarmDependencyErrorallarme viene chiamato.

Ti consigliamo vivamente di confermare la tua iscrizione a questo argomento SNS. Per ricevere messaggi pubblicati su un argomento, devi sottoscrivere un endpoint all'argomento. Per i dettagli, consulta Fase 1: Creare un argomento.

> **Note**
>
> Quando vengono creati allarmi di rilevamento delle anomalie, Alarm Manager crea automaticamente i modelli di rilevamento delle anomalie richiesti per le metriche specificate. Quando gli allarmi di rilevamento delle anomalie vengono eliminati, Alarm Manager non elimina i modelli di rilevamento delle anomalie associati.
> Amazon CloudWatch limita il numero di modelli di rilevamento delle anomalie che puoi avere in una determinata AWS regione. Se superi la quota del modello, Alarm Manager non crea nuovi allarmi di rilevamento delle anomalie. È necessario eliminare i modelli non utilizzati o collaborare con il proprio partner AMS per richiedere un aumento del limite.
> Molte delle definizioni di allarmi di base fornite da AMS Accelerate elencano l'argomento SNS, argomento MMS, come obiettivo. Viene utilizzato nel servizio di monitoraggio AMS Accelerate ed è il meccanismo di trasporto delle notifiche di allarme che arrivano ad AMS Accelerate. Non specificate l'argomento MMS come destinazione per eventuali allarmi diversi da quelli forniti nella baseline (e sostituzioni delle stesse), poiché il servizio ignora gli allarmi sconosciuti. Ciò non comporta che AMS Accelerate agisca sugli allarmi personalizzati.

Accelera il profilo di configurazione: sostituzione di pseudoparametri

In entrambi i profili di configurazione, è possibile specificare pseudoparametri che vengono sostituiti come segue:

- Globale: in qualsiasi punto del profilo:
  - $ {AWS::AccountId}: sostituito con l'ID AWS del tuo account
  - $ {AWS::Partition}: Sostituita con la partizione Regione AWS della risorsa is in (questa è 'aws' per la maggior parte Regioni AWS); per maggiori informazioni, vedi la voce per la partizione nel riferimento ARN.
  - $ {AWS::Region}: sostituito con il nome della regione in cui viene distribuita la risorsa (ad esempio us-east-1)
- In un blocco di tipo di AWS::EC2::Instancerisorsa:

  - $ {EC2::InstanceId}: (identifier) sostituito dall'ID di istanza della tua istanza Amazon EC2.
  - $ {EC2::InstanceName}: sostituito dal nome della tua istanza Amazon EC2. Se il nome dell'istanza non è definito, sostituito dall'ID dell'istanza Amazon EC2.
- In un blocco di tipo di risorsa AWS::EC2::Instance: :Disk:
  - $ {EC2::InstanceId}: (identifier) Sostituito dall'ID di istanza della tua istanza Amazon EC2.
  - $ {EC2::InstanceName}: Sostituito dal nome della tua istanza Amazon EC2. Se il nome dell'istanza non è definito, sostituito dall'ID dell'istanza Amazon EC2.
  - $ {EC2: :Disk: :Device}: Sostituito dal nome del disco. (Solo Linux, su istanze gestite dall'agente). CloudWatch
  - $ {EC2: :Disk::FSType}: Sostituito dal tipo di file system del disco. (Solo Linux, su istanze gestite da). CloudWatchAgent
  - $ {EC2: :Disk: :Path}: sostituito dal percorso del disco. (Solo per Windows, questa è l'etichetta dell'unità (ad esempio, c:/), solo su un'istanza gestita dall'CloudWatch agente).
  - $ {EC2: :Disk: :UUID}: (identifier) Sostituito da un UUID generato che identifica in modo univoco il disco, questo deve essere specificato nel nome dell'allarme, poiché un allarme in un tipo di risorsa creerà un allarme per volume. AWS::EC2::Instance::Disk Specificando $ {EC2: :Disk: :UUID} si mantiene l'unicità dei nomi degli allarmi.
- In un blocco di tipo di risorsa: AWS::OpenSearch::Domain
  - $ {OpenSearch::DomainName}: (identifier) sostituito dal nome del tuo OpenSearch dominio.
- In un blocco di tipo di AWS::Elasticsearch::Domainrisorsa:
  - $ {Elasticsearch::DomainName}: (identifier) sostituito dal nome del tuo dominio Elasticsearch.
- In un blocco di tipo di risorsa: AWS::ElasticLoadBalancing::LoadBalancer
  - $ {ElasticLoadBalancing:LoadBalancer: :Name}: (identifier) sostituito dal nome del tuo V1 Load Balancer.
- In un blocco di tipo di risorsa AWS::ElasticLoadBalancingV2::LoadBalancer:
  - $ {ElasticLoadBalancingV2:: :Arn}LoadBalancer: sostituito dall'ARN del tuo Load Balancer V2.
  - $ {ElasticLoadBalancingV2::LoadBalancer}: sostituito dall'ARN del tuo Load Balancer V2.
  - $ {ElasticLoadBalancingV2:LoadBalancer: :Name}: (identifier) sostituito dal nome del Load Balancer V2.
  - $ {ElasticLoadBalancingV2:::LoadBalancer:FullName}: sostituito dal nome completo del tuo Load Balancer V2.
- In un blocco di AWS::ElasticLoadBalancingV2::LoadBalancertipo di TargetGroup risorsa::

  - $ {ElasticLoadBalancingV2:::TargetGroup:FullName}: (identifier) sostituito dal nome del gruppo target del Load Balancer V2.
  - $ {ElasticLoadBalancingV2:: :UUID}TargetGroup: (identifier) sostituito da un UUID generato per il tuo Load Balancer V2.
  - $ {ElasticLoadBalancingV2:::LoadBalancer:FullName}: Sostituito dal nome completo del tuo Load Balancer V2.
- In un blocco di tipi di AWS::EC2::NatGatewayrisorse:
  - $ {NatGateway::NatGatewayId}: (identificatore) sostituito dal NAT Gateway ID.
- In un blocco di tipo di DBInstance risorsa AWS: :RDS::
  - $ {RDS:: DBInstance Identifier}: (identifier) sostituito dall'identificatore dell'istanza DB RDS.
- In un blocco di tipo di risorsa: AWS::Redshift::Cluster
  - $ {Redshift::ClusterIdentifier}: (identifier) sostituito dal tuo identificatore del cluster Redshift.
- In un blocco di tipo di VPNConnection risorsa AWS: :EC2::
  - $ {AWS::EC2::VpnConnectionId}: (identificatore) sostituito dal tuo ID VPN.
- In un blocco di tipo di AWS::EFS::FileSystemrisorsa:
  - $ {EFS::FileSystemId}: (identifier) Sostituito dall'ID del file system EFS.
- In un blocco di AWS::FSx::FileSystemtipo di risorsa: :ONTAP:
  - $ {FSx::FileSystemId}: (identifier) Sostituito dall'ID del file system del filesystem FSX.
  - $ {FSx::: :Throughput}FileSystem: Sostituito dal throughput del file system FSX.
  - $ {FSx:: :Iops}FileSystem: Sostituito dagli IOPS del file system FSX.
- In un blocco di tipo di risorsa AWS::FSx::FileSystem: :ONTAP: :Volume:
  - $ {FSx::FileSystemId}: (identifier) Sostituito dall'ID del file system del file system FSX.
  - $ {FSx: :ONTAP::VolumeId}: (identifier) Sostituito dall'ID del volume.
- In un blocco di tipo di AWS::FSx::FileSystemrisorsa: :Windows:
  - $ {FSx::FileSystemId}: (identifier) Sostituito dall'ID del file system del file system FSX.
  - $ {FSx::FileSystem: :Throughput}: Sostituito dal throughput del file system FSX.

> **Note**
>
> Tutti i parametri contrassegnati con l'identificatore vengono utilizzati come prefisso per il nome degli allarmi creati, a meno che non si specifichi tale identificatore nel nome dell'allarme.

Esempi di configurazione degli allarmi di accelerazione

Nell'esempio seguente, il sistema crea un allarme per ogni disco collegato all'istanza Linux corrispondente.

```
{
    "AWS::EC2::Instance::Disk": {
        "LinuxDiskAlarm": {
            "Tag": {
                "Key": "ams:rt:mylinuxinstance",
                "Value": "true"
            },
            "AlarmDefinition": {
                "MetricName": "disk_used_percent",
                "Namespace": "CWAgent",
                "Dimensions": [
                    {
                        "Name": "InstanceId",
                        "Value": "${EC2::InstanceId}"
                    },
                    {
                        "Name": "device",
                        "Value": "${EC2::Disk::Device}"
                    },
                    {
                        "Name": "fstype",
                        "Value": "${EC2::Disk::FSType}"
                    }
                ],
                "AlarmName": "${EC2::InstanceId}: Disk Usage Too High -
 ${EC2::Disk::UUID}"
                ...
            }
        }
    }
```

```
}
```

Nell'esempio seguente, il sistema crea un allarme per ogni disco collegato all'istanza Windows corrispondente.

```
{
     "AWS::EC2::Instance::Disk": {
        "WindowsDiskAlarm": {
            "Tag": {
                "Key": "ams:rt:mywindowsinstance",
                "Value": "true"
            },
            "AlarmDefinition": {
                "MetricName": "LogicalDisk % Free Space",
                "Namespace": "CWAgent",
                "Dimensions": [
                    {
                        "Name": "InstanceId",
                        "Value": "${EC2::InstanceId}"
                    },
                    {
                        "Name": "objectname",
                        "Value": "LogicalDisk"
                    },
                    {
                        "Name": "instance",
                        "Value": "${EC2::Disk::Path}"
                    }
                ],
                "AlarmName": "${EC2::InstanceId}: Disk Usage Too High -
 ${EC2::Disk::UUID}"
                ...
            }
        }
    }
}
```

Visualizzazione della configurazione di Accelerate Alarm Manager

Entrambi gli AMSManagedallarmi CustomerManagedAlarmspossono essere AppConfig esaminati GetConfigurationin.

Di seguito è riportato un esempio di `GetConfiguration` chiamata:

```
aws appconfig get-configuration --application AMSAlarmManager --environment
 AMSInfrastructure --configuration AMSManagedAlarms --client-id
      any-string outfile.json
```

- Applicazione: questa AppConfig è l'unità logica che fornisce funzionalità; per Alarm Manager, questa è `AMSAlarmManager`
- Ambiente: questo è l' AMSInfrastructure ambiente
- Configurazione: per visualizzare gli allarmi di base di AMS Accelerate, il valore è`AMSManagedAlarms`; per visualizzare le definizioni degli allarmi dei clienti, la configurazione è `CustomerManagedAlarms`
- ID client: si tratta di un identificatore univoco dell'istanza dell'applicazione, che può essere una stringa qualsiasi
- Le definizioni degli allarmi possono essere visualizzate nel file di output specificato, che in questo caso è `outfile.json`

Puoi vedere quale versione di configurazione è stata distribuita sul tuo account visualizzando le distribuzioni precedenti nell'ambiente. AMSInfrastructure

Modifica della configurazione dell'allarme Accelerate

Per aggiungere o aggiornare nuove definizioni di allarme, puoi distribuire il documento Utilizzo CloudFormation per implementare Accelerate le modifiche alla configurazione di configurazione o richiamare l'CreateHostedConfigurationVersionAPI.

Si tratta di un comando da riga di comando Linux che genera il valore del parametro in base64, che è ciò che il comando AppConfig CLI si aspetta. Per informazioni, consultate la AWS CLI documentazione, Binary/Blob (binary large object).

Ad esempio:

```
aws appconfig create-hosted-configuration-version --application-id application-id --
configuration-profile-id configuration-profile-id --content base64-string
      --content-type application/json
```

- ID dell'applicazione: ID dell'applicazione AMS AlarmManager; puoi scoprirlo con la chiamata API. ListApplications

- ID del profilo di configurazione: ID della configurazione CustomerManagedAlarms; puoi scoprirlo con la chiamata ListConfigurationProfilesAPI.
- Contenuto: stringa Base64 del contenuto, da creare creando un documento e codificandolo in base64: cat alarms-v2.json | base64 (vedi Binary/Blob (binary large object)).

  Tipo di **`application/json`**contenuto: tipo MIME, perché le definizioni degli allarmi sono scritte in JSON.

> **Important**
>
> Limita l'accesso alle azioni StartDeploymente alle StopDeploymentAPI a utenti fidati che comprendono le responsabilità e le conseguenze dell'implementazione di una nuova configurazione per i tuoi obiettivi.

Per ulteriori informazioni su come utilizzare le AppConfig funzionalità di AWS per creare e distribuire una configurazione, consulta Working with AWS AppConfig.

Modifica della configurazione predefinita di Accelerate alarm

Sebbene non sia possibile modificare il profilo di configurazione predefinito, è possibile sostituire i valori predefiniti specificando un blocco di configurazione nel profilo di personalizzazione con lo stesso ConfigurationID del blocco di configurazione predefinito. In tal caso, l'intero blocco di configurazione sovrascrive il blocco di configurazione predefinito a cui applicare la configurazione di etichettatura.

Ad esempio, considerate il seguente profilo di configurazione predefinito:

```
{
    "AWS::EC2::Instance": {
        "AMSManagedBlock1": {
            "Enabled": true,
            "Tag": {
                "Key": "ams:rt:ams-monitoring-policy",
                "Value": "ams-monitored"
            },
            "AlarmDefinition": {
                "AlarmName": "${EC2::InstanceId}: AMS Default Alarm",
                "Namespace": "AWS/EC2",
```

```
                "MetricName": "CPUUtilization",
                "Dimensions": [
                    {
                        "Name": "InstanceId",
                        "Value": "${EC2::InstanceId}"
                    }
                ],
                "Threshold": 5,
                ...
            }
        }
    }
}
```

Per modificare la soglia di questo allarme a 10, è necessario fornire l'intera definizione di allarme, non solo le parti che si desidera modificare. Ad esempio, potresti fornire il seguente profilo di personalizzazione:

```
{
    "AWS::EC2::Instance": {
        "AMSManagedBlock1": {
            "Enabled": true,
            "Tag": {
                "Key": "ams:rt:ams-monitoring-policy",
                "Value": "ams-monitored"
            },
            "AlarmDefinition": {
                "AlarmName": "${EC2::InstanceId}: AMS Default Alarm",
                "Namespace": "AWS/EC2",
                "MetricName": "CPUUtilization",
                "Dimensions": [
                    {
                        "Name": "InstanceId",
                        "Value": "${EC2::InstanceId}"
                    }
                ],
                "Threshold": 10,
                ...
            }
        }
    }
}
```

> **Important**
>
> Ricordati di implementare le modifiche alla configurazione dopo averle apportate. In SSM AppConfig, è necessario distribuire una nuova versione della configurazione dopo averla creata.

Implementazione delle modifiche alla configurazione di Accelerate

Dopo aver completato una personalizzazione, è necessario distribuirla con o. AppConfig CloudFormation

Argomenti

- Utilizzo AppConfig per implementare Accelerate le modifiche alla configurazione degli allarmi
- Utilizzo CloudFormation per implementare Accelerate le modifiche alla configurazione

Utilizzo AppConfig per implementare Accelerate le modifiche alla configurazione degli allarmi

Una volta completata la personalizzazione, utilizzala AppConfig per distribuire le modifiche con. StartDeployment

```
  aws appconfig start-deployment --application-id application_id
   --environment-id environment_id Vdeployment-strategy-id
   deployment_strategy_id --configuration-profile-id configuration_profile_id --
configuration-version 1
```

- ID applicazione: ID dell'applicazione`AMSAlarmManager`, puoi trovarlo con la chiamata ListApplicationsAPI.
- ID ambiente: puoi trovarlo con la chiamata ListEnvironmentsAPI.
- ID della strategia di implementazione: puoi trovarlo con la chiamata ListDeploymentStrategiesAPI.
- ID del profilo di configurazione: ID di`CustomerManagedAlarms`; puoi trovarlo con la chiamata ListConfigurationProfilesAPI.
- Versione di configurazione: la versione del profilo di configurazione da distribuire.

> **Important**
>
> Alarm Manager applica le definizioni degli allarmi come specificato nei profili di configurazione. Qualsiasi modifica manuale apportata agli CloudWatch allarmi con Console di gestione AWS o CloudWatch CLI/SDK viene ripristinata automaticamente, quindi assicurati che le modifiche siano definite tramite Alarm Manager. Per capire quali allarmi vengono creati da Alarm Manager, puoi cercare il tag con valore. `ams:alarm-manager:managed true` Limita l'accesso alle azioni StartDeployment e alle StopDeployment API a utenti fidati che comprendono le responsabilità e le conseguenze dell'implementazione di una nuova configurazione per i tuoi obiettivi.

Per ulteriori informazioni su come utilizzare le AppConfig funzionalità di AWS per creare e distribuire una configurazione, consulta la AppConfig documentazione AWS.

Utilizzo CloudFormation per implementare Accelerate le modifiche alla configurazione

Se desideri distribuire il tuo profilo di `CustomerManagedAlarms` configurazione utilizzando CloudFormation, puoi utilizzare i seguenti CloudFormation modelli. Inserisci la configurazione JSON desiderata nel `AMSAlarmManagerConfigurationVersion.Content` campo.

Quando distribuisci i modelli in uno CloudFormation stack o in uno stack set, la distribuzione della `AMSResourceTaggerDeployment` risorsa avrà esito negativo se non hai seguito il formato JSON richiesto per la configurazione. Vedi Accelera il profilo di configurazione: monitoraggio per i dettagli sul formato previsto.

Per assistenza sulla distribuzione di questi modelli come CloudFormation stack o set di stack, consulta la documentazione CloudFormation AWS pertinente di seguito:

- Creazione di uno stack sulla console AWS CloudFormation
- Creazione di uno stack con AWS CLI
- Creazione di un set di stack

> **Note**
>
> Se si distribuisce una versione di configurazione utilizzando uno di questi modelli e successivamente si elimina lo CloudFormation stack/stack set, la versione di configurazione del modello rimarrà la versione attualmente distribuita e non verrà effettuata alcuna

distribuzione aggiuntiva. Se desideri tornare a una configurazione predefinita, dovrai distribuire manualmente una configurazione vuota (ad esempio solo {}) o aggiornare lo stack a una configurazione vuota, anziché eliminare lo stack.

JSON

```
{
  "Description": "Custom configuration for the AMS Alarm Manager.",
  "Resources": {
    "AMSAlarmManagerConfigurationVersion": {
      "Type": "AWS::AppConfig::HostedConfigurationVersion",
      "Properties": {
        "ApplicationId": {
          "Fn::ImportValue": "AMS-Alarm-Manager-Configuration-ApplicationId"
        },
        "ConfigurationProfileId": {
          "Fn::ImportValue": "AMS-Alarm-Manager-Configuration-CustomerManagedAlarms-
ProfileID"
        },
        "Content": "{}",
        "ContentType": "application/json"
      }
    },
    "AMSAlarmManagerDeployment": {
      "Type": "AWS::AppConfig::Deployment",
      "Properties": {
        "ApplicationId": {
          "Fn::ImportValue": "AMS-Alarm-Manager-Configuration-ApplicationId"
        },
        "ConfigurationProfileId": {
          "Fn::ImportValue": "AMS-Alarm-Manager-Configuration-CustomerManagedAlarms-
ProfileID"
        },
        "ConfigurationVersion": {
          "Ref": "AMSAlarmManagerConfigurationVersion"
        },
        "DeploymentStrategyId": {
          "Fn::ImportValue": "AMS-Alarm-Manager-Configuration-Deployment-StrategyID"
        },
        "EnvironmentId": {
          "Fn::ImportValue": "AMS-Alarm-Manager-Configuration-EnvironmentId"
        }
```

```
      }
    }
  }
}
```

YAML

```
Description: Custom configuration for the AMS Alarm Manager.
Resources:
  AMSAlarmManagerConfigurationVersion:
    Type: AWS::AppConfig::HostedConfigurationVersion
    Properties:
      ApplicationId:
        !ImportValue AMS-Alarm-Manager-Configuration-ApplicationId
      ConfigurationProfileId:
        !ImportValue AMS-Alarm-Manager-Configuration-CustomerManagedAlarms-ProfileID
      Content: |
        {

        }
      ContentType: application/json
  AMSAlarmManagerDeployment:
    Type: AWS::AppConfig::Deployment
    Properties:
      ApplicationId:
        !ImportValue AMS-Alarm-Manager-Configuration-ApplicationId
      ConfigurationProfileId:
        !ImportValue AMS-Alarm-Manager-Configuration-CustomerManagedAlarms-ProfileID
      ConfigurationVersion:
        !Ref AMSAlarmManagerConfigurationVersion
      DeploymentStrategyId:
        !ImportValue AMS-Alarm-Manager-Configuration-Deployment-StrategyID
      EnvironmentId:
        !ImportValue AMS-Alarm-Manager-Configuration-EnvironmentId
```

Rolling back Accelera le modifiche agli allarmi

È possibile ripristinare le definizioni degli allarmi tramite lo stesso meccanismo di distribuzione specificando una versione precedente del profilo di configurazione ed StartDeployment eseguendola.

Mantenimento degli allarmi Accelerate

Quando le risorse monitorate da AMS vengono eliminate, tutti gli allarmi creati da Alarm Manager per tali risorse vengono eliminati automaticamente da Alarm Manager. Se è necessario conservare determinati allarmi per scopi di controllo, conformità o cronologia, utilizza la funzionalità di mantenimento dei tag di memorizzazione di Alarm Manager.

Per mantenere un avviso anche dopo l'eliminazione della relativa risorsa monitorata, aggiungi un `"ams:alarm-manager:retain"` tag alla configurazione personalizzata dell'avviso, come mostrato nell'esempio seguente.

```
{
  "AWS::EC2::Instance": {
    "AMSCpuAlarm": {
      "Enabled": true,
      "Tag": {
        "Key": "ams:rt:ams-monitoring-policy",
        "Value": "ams-monitored"
      },
      "AlarmDefinition": {
        "AlarmName": "${EC2::InstanceId}: CPU Too High",
        "AlarmDescription": "AMS Baseline Alarm for EC2 CPUUtilization",
        [...]
        "Tags": [
          {
            "Key": "ams:alarm-manager:retain",
            "Value": "true"
          }
        ]
      }
    }
  }
}
```

Un allarme configurato con il `"ams:alarm-manager:retain"` tag non viene eliminato automaticamente da Alarm Manager quando la risorsa monitorata viene terminata. L'allarme mantenuto persiste a CloudWatch tempo indeterminato fino a quando non viene rimosso manualmente utilizzando. CloudWatch

Disattivazione della configurazione predefinita di Accelerate alarm

AMS Accelerate fornisce il profilo di configurazione predefinito nell'account in base agli allarmi di base. Tuttavia, questa configurazione predefinita può essere disabilitata sovrascrivendo una qualsiasi delle definizioni di allarme. È possibile disabilitare una regola di configurazione predefinita sovrascrivendo il ConfigurationID della regola nel profilo di configurazione di personalizzazione e specificando il campo enabled con il valore false.

Ad esempio, se nel profilo di configurazione predefinito era presente la seguente configurazione:

```
{
    "AWS::EC2::Instance": {
        "AMSManagedBlock1": {
            "Enabled": true,
            "Tag": {
                "Key": "ams:rt:ams-monitoring-policy",
                "Value": "ams-monitored"
            },
            "AlarmDefinition": {
                ...
            }
        }
    }
```

È possibile disabilitare questa regola di etichettatura includendo quanto segue nel profilo di configurazione di personalizzazione:

```
{
    "AWS::EC2::Instance": {
        "AMSManagedBlock1": {
            "Enabled": false
        }
    }
}
```

Per apportare queste modifiche, l'CreateHostedConfigurationVersionAPI deve essere chiamata con il documento del profilo JSON (vediModifica della configurazione dell'allarme Accelerate) e successivamente deve essere distribuita (vedi). Implementazione delle modifiche alla configurazione di Accelerate Tieni presente che quando crei la nuova versione di configurazione, devi includere anche tutti gli allarmi personalizzati creati in precedenza che desideri nel documento del profilo JSON.

> **Important**
>
> Quando AMS Accelerate aggiorna il profilo di configurazione predefinito, non viene calibrato in base agli allarmi personalizzati configurati, quindi rivedi le modifiche agli allarmi predefiniti quando le sovrascrivi nel tuo profilo di configurazione di personalizzazione.

Creazione di CloudWatch allarmi aggiuntivi per Accelerate

Puoi creare CloudWatch allarmi aggiuntivi per AMS Accelerate utilizzando CloudWatch metriche e allarmi personalizzati per le istanze Amazon. EC2

Produci lo script di monitoraggio delle applicazioni e i parametri personalizzati. Per ulteriori informazioni e accesso a script di esempio, consulta Monitoring Memory and Disk Metrics EC2 for Amazon Linux Instances.

Gli script di CloudWatch monitoraggio per le EC2 istanze Linux Amazon dimostrano come produrre e utilizzare metriche personalizzate CloudWatch . Questi script Perl di esempio contengono un esempio completamente funzionale che crea report sui parametri di memoria, swap e uso dello spazio su disco relativi a un'istanza Linux.

> **Important**
>
> AMS Accelerate non monitora gli CloudWatch allarmi creati dall'utente.

Correzione automatica degli avvisi con AMS

Dopo la verifica, AWS Managed Services (AMS) corregge automaticamente determinati avvisi in base a condizioni e processi specifici descritti in questa sezione.

Nome dell'avviso	Description	Soglie	Azione
Controllo dello stato non riuscito	Possibili guasti hardware o stato di errore dell'istanza.	Il sistema ha rilevato uno stato di errore almeno una volta negli ultimi 15 minuti.	La riparazione automatica AMS verifica innanzitutto se l'istanza è accessibile. Se l'istanza è inaccessi

Nome dell'avviso	Description	Soglie	Azione
			bile, viene interrotta e riavviata. L'arresto e l'avvio consentono all'istanza di migrare verso il nuovo hardware sottostante. Per ulteriori informazioni, consulta la seguente sezione «EC2 Status Check Failure Remediation Automatio n».
AMSLinuxDiskUsage	Si attiva quando l'utilizzo del disco di 1 punto di montaggio (spazio designato su un volume) sull'istanza EC2 si sta esaurendo.	La soglia supera il valore definito 6 volte negli ultimi 30 minuti.	La riparazione automatica AMS elimina innanzitutto i file temporanei. Se ciò non libera abbastanza spazio su disco, estende il volume per evitare tempi di inattività se il volume si riempie.
AMSWindowsDiskUsage	Quando l'utilizzo del disco di 1 punto di montaggio (spazio designato su un volume) sull'istanza EC2 si sta esaurendo.	La soglia supera il valore definito 6 volte negli ultimi 30 minuti.	La riparazione automatica AMS elimina innanzitutto i file temporanei. Se ciò non libera abbastanza spazio su disco, estende il volume per evitare tempi di inattività se il volume si riempie.

Nome dell'avviso	Description	Soglie	Azione
RDS-EVENT-0089	L'istanza database ha utilizzato oltre il 90% dello storage allocato.	Lo spazio di archiviazione è allocato per oltre il 90%.	La correzione automatica AMS verifica innanzitutto che il DB sia in uno stato modificabile e disponibile o che lo spazio di archiviazione sia pieno. Tenta quindi di aumentare lo storage allocato, gli IOPS e il throughput di storage tramite un changeset. CloudFormation Se è già stata rilevata una deriva dello stack, ricorre all'API RDS per evitare tempi di inattività. Questa funzionalità può essere disattivata aggiungendo il seguente tag all'istanza DB RDS: `"Key: ams:rt:ams-rds-max-allocated-storage-policy, Value: ams-opt-out".`

Nome dell'avviso	Description	Soglie	Azione
RDS-EVENT-0007	Lo storage allocato per l'istanza DB è esaurito. Per risolvere, alloca spazio di archiviazione aggiuntivo.	Lo storage è allocato al 100%.	La correzione automatica AMS verifica innanzitutto che il DB sia in uno stato modificabile e disponibile o che lo spazio di archiviazione sia pieno. Tenta quindi di aumentare lo storage allocato, gli IOPS e il throughput di storage tramite un changeset. CloudFormation Se è già stata rilevata una deriva dello stack, ricorre all'API RDS per evitare tempi di inattività. Questa funzionalità può essere disattivata aggiungendo il seguente tag all'istanza DB RDS: `"Key: ams:rt:ams-rds-max-allocated-storage-policy, Value: ams-opt-out".`

Nome dell'avviso	Description	Soglie	Azione
RDS-EVENT-0224	Lo storage allocato richiesto raggiunge o supera la soglia di archiviazione massima configurata.	La soglia massima di archiviazione per l'istanza DB è stata esaurita o è maggiore o uguale allo storage allocato richiesto.	La riparazione automatica AMS verifica innanzitutto che la quantità richiesta di storage RDS superi la soglia massima di archiviazione. Se confermata, AMS tenta di aumentare la soglia massima di archiviazione del 30% con un CloudFormation changeset o un'API RDS diretta se le risorse non vengono fornite tramite. CloudFormation Questa funzionalità può essere disattivata aggiungendo il seguente tag all'istanza DB RDS: `"Key: ams:rt:ams-rds-max-allocated-storage-policy, Value: ams-opt-out".`

Nome dell'avviso	Description	Soglie	Azione
Capacità di archiviazione RDS	Rimane meno di 1 GB nello storage allocato per l'istanza DB.	Lo storage è allocato al 99%.	La correzione automatica AMS verifica innanzitutto che il DB sia in uno stato modificabile e disponibile o che lo spazio di archiviazione sia pieno. Tenta quindi di aumentare lo storage allocato, gli IOPS e il throughput di storage tramite un changeset. CloudFormation Se è già stata rilevata una deriva dello stack, ricorre all'API RDS per evitare tempi di inattività. Questa funzionalità può essere disattivata aggiungendo il seguente tag all'istanza DB RDS: `"Key: ams:rt:ams-rds-max-allocated-storage-policy, Value: ams-opt-out".`

Nome dell'avviso	Description	Soglie	Azione
AMSFSXONTAPVolumeCapacityUtilization	Il volume Amazon FSx for NetApp ONTAP ha consumato più dello storage allocato predefinito (80%).	FSx per ONTAP l'utilizzo della capacità di volume è superiore all'80% per due ore (valore predefinito).	La correzione automatica AMS verifica innanzitutto che lo stato del ciclo di vita del volume sia in uno stato modificabile, quindi estende le dimensioni del volume del 10% verificando la capacità massima del file system. Se il file system non dispone di una capacità di archiviazione sufficiente per l'espansione del volume, sia il volume che il file system vengono espansi insieme. Questa espansione è limitata a un massimo di tre volte nell'arco di sette giorni. Il limite massimo di storage a cui si espande AMS Automation è di 5120 GiB. **Note** Se il LUN iSCSI è configurato nella parte superiore del volume, espandere il LUN iSCSI a livello di sistema operativo. Per ulteriori

Nome dell'avviso	Description	Soglie	Azione
			informazioni, vedi Perché my FSx for ONTAP LUN è in modalità di sola lettura?

Errore nel controllo dello stato di EC2: note sull'automazione della riparazione

Come funziona la riparazione automatica di AMS con i problemi relativi al controllo dello stato di EC2:

- Se la tua istanza Amazon EC2 è diventata irraggiungibile, l'istanza deve essere interrotta e riavviata in modo da poter essere migrata su un nuovo hardware e ripristinata.
- Se la radice del problema è all'interno del sistema operativo (dispositivi mancanti in fstab, danneggiamento del kernel e così via), l'automazione non è in grado di ripristinare l'istanza.
- Se l'istanza appartiene a un gruppo Auto Scaling, l'automazione non interviene: l'azione di AutoScalingGroup ridimensionamento sostituisce l'istanza.
- Se la tua istanza ha EC2 Auto Recovery abilitato, la riparazione non interviene.

Automazione della correzione dell'utilizzo dei volumi EC2

Come funziona la riparazione automatica di AWS Managed Services (AMS) con i problemi di utilizzo dei volumi EC2:

- L'automazione verifica innanzitutto se l'espansione del volume è necessaria e se può essere eseguita. Se l'espansione è ritenuta appropriata, l'automazione può aumentare la capacità del volume. Questo processo automatizzato bilancia l'esigenza di crescita con un'espansione controllata e limitata.
- Prima di estendere un volume, l'automazione esegue attività di pulizia (Windows: Disk Cleaner, Linux: Logrotate + rimozione del registro dell'agente di Simple Service Manager) sull'istanza per cercare di liberare spazio.

> **Note**
>
> Le attività di pulizia non vengono eseguite sulle istanze della famiglia EC2 «T» perché si affidano ai crediti della CPU per la continuità delle funzionalità.

- Su Linux, l'automazione supporta solo l'estensione dei file system di tipo EXT2 C e XFS. EXT3 EXT4
- Su Windows, l'automazione supporta solo New Technology File System (NTFS) e Resilient File System (ReFS).
- L'automazione non estende i volumi che fanno parte di Logical Volume Manager (LVM) o di un array RAID.
- L'automazione non estende i volumi dell'Instance Store.
- L'automazione non interviene se il volume interessato è già superiore a 2 TiB.
- L'espansione attraverso l'automazione è limitata a un massimo di tre volte alla settimana e cinque volte in totale nell'arco della vita del sistema.
- L'automazione non aumenta il volume se l'espansione precedente è avvenuta nelle ultime sei ore.

Quando queste regole impediscono all'automazione di agire, AMS ti contatta tramite una richiesta di servizio in uscita per determinare le azioni successive da intraprendere.

Automazione della correzione degli eventi a basso livello di storage di Amazon RDS

Come funziona la riparazione automatica di AWS Managed Services (AMS) con i problemi relativi agli eventi di storage insufficiente di Amazon RDS:

- Prima di provare a estendere lo storage dell'istanza Amazon RDS, l'automazione esegue diversi controlli per garantire che l'istanza Amazon RDS sia in uno stato modificabile e disponibile o pieno di spazio di archiviazione.
- Se viene rilevata una deriva CloudFormation dello stack, la correzione avviene tramite l'API Amazon RDS.
- A seconda dell'evento scatenante, la riparazione modifica le proprietà,, o. `MaxAllocatedStorage` `AllocatedStorage` `Iops` `StorageThroughput` Le altre proprietà delle istanze Amazon RDS non vengono modificate. Per ulteriori informazioni, consulta Impostazioni per le istanze DB.

- L'azione di riparazione non viene eseguita nei seguenti scenari:
  - Lo stato dell'istanza Amazon RDS non è «disponibile» o «pieno di spazio di archiviazione».
  - Lo storage delle istanze Amazon RDS non è attualmente modificabile (ad esempio quando lo storage è stato modificato nelle ultime sei ore).
  - L'istanza Amazon RDS ha lo storage con scalabilità automatica abilitato.
- La riparazione è limitata a un'espansione ogni sei ore e a non più di tre espansioni nell'arco di quattordici giorni consecutivi.
- Quando si verificano questi scenari, AMS ti contatta per segnalarti un incidente in uscita per determinare le azioni successive.

Automazione della riparazione della capacità dei volumi ONTAP

Come funziona la riparazione automatica di AWS Managed Services (AMS) con i problemi di capacità dei volumi ONTAP:

- Prima di estendere il volume, l'automazione verifica che lo stato del ciclo di vita del volume sia in uno stato modificabile.
- L'automazione estende la dimensione del volume del 10% verificando al contempo la capacità massima del file system.
- Se il file system non dispone di una capacità di archiviazione sufficiente per supportare l'espansione del volume, viene aumentata sia la capacità del volume che quella del file system.
- La riparazione è limitata a non più di tre aggiornamenti in un periodo di sette giorni.
- Il limite massimo di storage a cui si espande AMS Automation è di 5120 GiB.
- Se il LUN iSCSI è configurato sulla parte superiore del volume, è necessario espandere manualmente il LUN iSCSI a livello di sistema operativo dopo il completamento della riparazione automatica. Per ulteriori informazioni, vedi Perché my for ONTAP LUN è in modalità di sola FSx lettura?

Utilizzo di Amazon EventBridge Managed Rules in AMS

AMS Accelerate utilizza Amazon EventBridge Managed Rules. Una Managed Rule è un tipo di regola unico direttamente collegato ad AMS. Queste regole corrispondono agli eventi in arrivo e li inviano alle destinazioni per l'elaborazione. Le Managed Rules sono predefinite da AMS e includono i modelli

di eventi richiesti dal servizio per gestire gli account dei clienti e, se non diversamente definito, solo il servizio proprietario può utilizzare queste Managed Rules.

Le regole gestite di AMS Accelerate sono collegate al `events.managedservices.amazonaws.com` responsabile del servizio. Queste Managed Rules sono gestite tramite il ruolo `AWSServiceRoleForManagedServices_Events`collegato al servizio. Per eliminare queste regole è necessaria una conferma speciale da parte del cliente. Per ulteriori informazioni, consulta Eliminazione delle regole gestite per AMS.

Per ulteriori informazioni sulle regole, consulta Rules nella Amazon EventBridge User Guide.

Amazon EventBridge Managed Rules implementato da AMS

Regole EventBridge gestite da Amazon

Nome regola	Description	Definizione

AmsAccessRolesRule	Questa regola tiene conto delle modifiche ai ruoli e alle politiche specifici di AMS Accelerate.	{
		"source": ["aws.iam"],
		"detail-type": ["AWS API Call via CloudTrail"],
		"detail": {
		"eventName": [
		"DeleteRole",
		"DeletePolicy",
		"CreatePolicyVersion",
		"AttachRolePolicy",
		"DetachRolePolicy"
		],
		"requestParameters": {
		"$or": [
		{
		"roleName": [
		"ams-access-admin",
		"ams-access-admin-operations",
		"ams-access-operations",
		"ams-access-read-only",
		"ams-access-security-analyst",
		"ams-access-security-analyst-read-only"
		]
		},

Nome regola	Description	Definizione

		<pre>{
		"policyArn": [
		"arn:*:iam::*:policy/ams-access-allow-pass-role",
		"arn:*:iam::*:policy/ams-access-deny-cloudshell-policy",
		"arn:*:iam::*:policy/ams-access-deny-operations-policy",
		"arn:*:iam::*:policy/ams-access-deny-update-iam-policy",
		"arn:*:iam::*:policy/ams-access-ssr-policy",
		"arn:*:iam::*:policy/ams-access-security-analyst-read-only-policy",
		"arn:*:iam::*:policy/ams-access-security-analyst-policy",
		"arn:*:iam::*:policy/ams-access-security-analyst-extended-policy",
		"arn:*:iam::*:policy/ams-access-admin-policy",
		"arn:*:iam::*:policy/ams-access-admin-operations-policy"
		]
		},
		]
		},
		},
		}</pre>

Nome regola	Description	Definizione

AMSCoreRegola	Questa regola inoltra CloudWatch gli eventi Amazon ai servizi di correzione AWS Config e monitoraggio AMS Config rispettosamente. Gli AWS Config eventi si creano e si risolvono. AWS Systems Manager OpsItems Gli CloudWatch eventi di Amazon monitorano gli CloudWatch allarmi.	<pre>{
		    {
		        "source": ["aws.config", "aws.cloudwatch"],
		        "detail-type": ["Config Rules Compliance Change", "CloudWatch Alarm State Change"],
		    }
		}</pre>

Creazione di regole gestite per AMS

Non è necessario creare manualmente Amazon EventBridge Managed Rules. Quando effettui l'onboarding su AMS tramite la console di AWS gestione AWS CLI, l'API o l' AWS API, AMS le crea per te.

Modifica delle regole gestite per AMS

AMS non consente di modificare le Managed Rules. Il nome e lo schema di eventi per ogni Managed Rule sono predefiniti da AMS.

Eliminazione delle regole gestite per AMS

Non è necessario eliminare manualmente le Managed Rules. Quando esci da AMS tramite la Console di AWS gestione, l'API o l' AWS API AWS CLI, AMS ripulisce le risorse ed elimina tutte le Managed Rules di proprietà di AMS per te.

Nel caso in cui AMS non riesca a rimuovere le Managed Rules durante l'offboarding, puoi anche utilizzare la EventBridge console Amazon, AWS CLI o l' AWS API per eliminare manualmente le Managed Rules. Per fare ciò, devi prima abbandonare AMS e procedere all'eliminazione forzata delle Managed Rules.

Trusted Remediator in AMS

Trusted Remediator è una soluzione AWS Managed Services che automatizza la correzione e le AWS Trusted Advisorraccomandazioni AWS Security Hub CSPM. AWS Compute Optimizer Trusted Remediator crea consigli quando Trusted Advisor Security Hub CSPM e Compute Optimizer indicano opportunità per ridurre i costi, migliorare la disponibilità del sistema, ottimizzare le prestazioni o colmare le lacune di sicurezza per voi. Account AWS Con Trusted Remediator, puoi rispondere a questi consigli su sicurezza, prestazioni, ottimizzazione dei costi, tolleranza agli errori e limiti di servizio in modo sicuro e standardizzato che utilizza le migliori pratiche consolidate. Trusted Remediator consente di configurare una soluzione di riparazione e viene eseguito automaticamente in base a una pianificazione creata dall'utente, semplificando il processo di riparazione. Questo approccio semplificato risolve i problemi in modo coerente, efficiente e senza interventi manuali.

Vantaggi principali di Trusted Remediator

Di seguito sono riportati i principali vantaggi di Trusted Remediator:

- Maggiore sicurezza, prestazioni e ottimizzazione dei costi: Trusted Remediator consente di migliorare il livello di sicurezza generale degli account, ottimizzare l'utilizzo delle risorse e ridurre i costi operativi.
- Configurazione e configurazione self-service: è possibile configurare Trusted Remediator in base ai propri requisiti e preferenze.

- Trusted Advisor Controlli automatici, controlli CSPM di Security Hub e correzione dei AWS Compute Optimizer suggerimenti: dopo la configurazione, Trusted Remediator esegue automaticamente le azioni di riparazione per i controlli selezionati. Questa automazione elimina la necessità di un intervento manuale.
- Implementazione delle migliori pratiche: le azioni correttive si basano su best practice consolidate, quindi i problemi vengono risolti in modo standardizzato ed efficace.
- Esecuzione pianificata: è possibile scegliere il programma di riparazione che si allinea ai flussi di lavoro operativi. day-to-day

Trusted Remediator ti consente di affrontare in modo proattivo i problemi identificati nei tuoi AWS ambienti, aiutandoti a rispettare le migliori pratiche e a mantenere un'infrastruttura cloud sicura, ad alte prestazioni ed economica.

Come funziona Trusted Remediator

Di seguito è riportato un esempio del flusso di lavoro Trusted Remediator:

Trusted Remediator valuta Trusted Advisor, consiglia Security Hub CSPM e Compute Optimizer per te e crea. Account AWS AWS Systems Manager OpsItems OpsCenter Quindi, è possibile utilizzare i documenti di automazione Trusted Remediator per rimediare automaticamente o manualmente. OpsItems Di seguito sono riportati i dettagli per ogni tipo di riparazione:

- Riparazione automatica: Trusted Remediator esegue il documento di automazione e monitora l'esecuzione. Una volta completato il documento di automazione, Trusted Remediator risolve l'Opsitem.
- Riparazione manuale: Trusted Remediator crea il file da esaminare. OpsItem Dopo la revisione, si avvia il documento di automazione.

I log di riparazione sono archiviati in un bucket Amazon S3. Puoi utilizzare i dati nel bucket S3 per creare dashboard Quick personalizzati per la reportistica. AMS fornisce anche report su richiesta per Trusted Remediator. Per ricevere questi report, contattate il vostro CSDM. Per ulteriori informazioni, consulta Report di Trusted Remediator.

Termini chiave per Trusted Remediator

Di seguito sono riportati i termini che è utile conoscere quando si utilizza Trusted Remediator in AMS:

- AWS Trusted Advisor AWS Security Hub e AWS Compute Optimizer: Servizi di ottimizzazione del cloud forniti da AWS. Trusted Advisor, Security Hub CSPM e Compute Optimizer ispezionano AWS l'ambiente e forniscono consigli basati sulle migliori pratiche nelle seguenti sei categorie:
  - Ottimizzazione dei costi
  - Performance
  - Sicurezza
  - Tolleranza ai guasti
  - Eccellenza operativa
  - Limiti del servizio

  Per ulteriori informazioni, vedere, e. AWS Trusted AdvisorAWS Security HubAWS Compute Optimizer
- Trusted Remediator: una soluzione di correzione AMS per Trusted Advisorcontrolli, AWS Security Hub CSPMraccomandazioni e AWS Compute Optimizerraccomandazioni. Trusted Remediator ti aiuta a correggere in sicurezza i Trusted Advisor controlli, i controlli CSPM di Security Hub e le raccomandazioni di Compute Optimizer con le migliori pratiche note per migliorare la sicurezza, le prestazioni e ridurre i costi. Trusted Remediator è facile da configurare e configurare. La configurazione viene effettuata una sola volta e Trusted Remediator esegue le riparazioni secondo la pianificazione preferita (giornaliera o settimanale).
- AWS Systems Manager Documento SSM: un file JSON o YAML che definisce le azioni eseguite sulle risorse. AWS Systems Manager AWS Il documento SSM funge da specifica dichiarativa per automatizzare le attività operative su più risorse e istanze. AWS
- AWS Systems Manager OpsCenter OpsItem: Una risorsa per la gestione dei problemi operativi nel cloud che ti aiuta a tracciare e risolvere i problemi operativi nel tuo ambiente. AWS OpsItems forniscono un sistema di visualizzazione e gestione centralizzato dei dati e dei problemi operativi su tutte Servizi AWS le risorse. Ciascuno di essi OpsItem rappresenta un problema operativo, ad esempio un potenziale rischio per la sicurezza, un problema di prestazioni o un incidente operativo.
- Configurazione: una configurazione è un insieme di attributi archiviati in AWS AppConfig, una capacità di AWS Systems Manager. L'applicazione Trusted Remediator AWS AppConfig aiuta a configurare le riparazioni a livello di account. È possibile utilizzare la AWS AppConfig console o l'API per modificare le configurazioni.
- Modalità di esecuzione: la modalità di esecuzione è un attributo di configurazione che determina come eseguire la correzione per ogni risultato di Trusted Advisor controllo e i consigli di Compute Optimizer e Security Hub CSPM. Sono supportate quattro modalità di esecuzione: automatizzata, manuale, condizionale, inattiva.

- Sostituzione delle risorse: questa funzionalità utilizza i tag delle risorse per sovrascrivere una configurazione per risorse specifiche.
- Registro degli elementi di riparazione: un file di registro nel bucket di registro S3 di Trusted Remediator remediation. Il registro degli elementi di riparazione viene creato al momento della creazione della riparazione. OpsItems Questo file di registro contiene la correzione manuale dell'esecuzione OpsItems e la riparazione automatica dell'esecuzione. OpsItems Utilizzate questo file di registro per tenere traccia di tutti gli elementi di riparazione.
- Registro di esecuzione automatizzata della riparazione: un file di registro nel bucket di registro S3 di Trusted Remediator remediation. Il registro di esecuzione automatica della riparazione viene creato al termine dell'esecuzione automatizzata di un documento SSM. Questo registro contiene i dettagli di esecuzione SSM per la correzione automatica dell'esecuzione. OpsItems Utilizza questo file di registro per tenere traccia delle riparazioni automatiche.

Inizia a usare Trusted Remediator in AMS

Trusted Remediator è disponibile in AMS senza costi aggiuntivi. Trusted Remediator supporta configurazioni con account singolo e multiaccount.

Effettua l'integrazione su Trusted Remediator

Per effettuare l'onboarding dei tuoi account AMS su Trusted Remediator, invia un'e-mail ai tuoi Cloud Architect o ai Cloud Service Delivery Manager (). CSDMs Nell'e-mail, includi le seguenti informazioni:

- Account AWS: Il numero di identificazione dell'account a dodici cifre. Tutti gli account che desideri aggiungere a Trusted Remediator devono appartenere allo stesso cliente Accelerate.
  - Account amministratore delegato: l'account utilizzato per Trusted Advisor la configurazione di controllo CSPM di Compute Optimizer e Security Hub per uno o più account.
  - Account membro: questi sono gli account collegati all'account amministratore delegato. Questi account ereditano le configurazioni dall'account amministratore delegato. È possibile avere uno o più account membro.

> **Note**
>
> Gli account membro ereditano le configurazioni dall'account amministratore delegato. Se hai bisogno di configurazioni diverse per account specifici, esegui l'onboarding di più

account amministratore delegato con le tue configurazioni preferite. Pianifica la struttura dell'account e le configurazioni con i tuoi Cloud Architects prima di iniziare.

- Regioni AWS: Il Regioni AWS luogo in cui si trovano le tue risorse. Per un elenco di Regioni AWS, vedi Servizi AWS per regione.
- Pianificazione e orario di riparazione: il tuo programma di riparazione preferito (giornaliero o settimanale). Trusted Remediator raccoglie Trusted Advisor i controlli e avvia la riparazione all'ora pianificata. Ad esempio, è possibile impostare il programma di riparazione per l'1:00 di domenica di ogni settimana, ora solare dell'Australia orientale.
- E-mail di notifica: Trusted Remediator utilizza l'e-mail di notifica per avvisarti quotidianamente in caso di correzioni. L'oggetto dell'e-mail di notifica è «Riepilogo delle riparazioni di Trusted Remediator» e il contenuto fornisce informazioni sulle riparazioni di Trusted Remediator eseguite nelle ultime 24 ore.

> **Note**
>
> Esaminate le applicazioni e le risorse dopo ogni riparazione pianificata. Per ulteriore assistenza, contatta AMS.

Dopo aver inviato la richiesta di onboard con i dettagli richiesti alla CA o al CSDM, AMS effettua l'onboarding dei tuoi account su Trusted Remediator. Trusted Remediator utilizza AWS AppConfig, una funzionalità di AWS Systems Manager, per definire la configurazione per i controlli. Trusted Advisor Queste configurazioni sono un insieme di attributi che vengono memorizzati in. AWS AppConfig Per evitare addebiti non autorizzati alle risorse, tutti i Trusted Advisor controlli supportati sono impostati su Inattivo quando gli account vengono registrati su Trusted Remediator. Dopo l'onboarding, puoi utilizzare la AWS AppConfig console o l'API per gestire le configurazioni. Queste configurazioni consentono di correggere automaticamente Trusted Advisor controlli specifici o di valutare e correggere manualmente i controlli rimanenti. Le configurazioni sono altamente personalizzabili e consentono di applicare configurazioni per ogni controllo. Trusted Advisor Per ulteriori informazioni, consulta Configurare Trusted Advisor la correzione degli assegni in Trusted Remediator.

Scegli i controlli e i consigli per rimediare

Per impostazione predefinita, la modalità di esecuzione della riparazione è inattiva per tutti i Trusted Advisor controlli, i consigli di Compute Optimizer e i consigli CSPM di Security Hub nella

configurazione. In questo modo si evitano interventi di riparazione non autorizzati e si proteggono le risorse. AMS fornisce documenti di automazione SSM curati per la correzione degli assegni. Trusted Advisor

Per selezionare i controlli a cui desideri correggere con Trusted Remediator, completa i seguenti passaggi:

1. Consulta l'elenco delle raccomandazioni supportate Trusted Advisor, di Compute Optimizer, delle raccomandazioni CSPM di Security Hub e il nome dei documenti di automazione SSM associati per decidere quali controlli e consigli desideri correggere con Trusted Remediator.
2. Aggiorna la configurazione per attivare la correzione per i Trusted Advisor controlli selezionati, i consigli di Compute Optimizer e i consigli CSPM di Security Hub. Per istruzioni su come selezionare i controlli, consulta. Configurare Trusted Advisor la correzione degli assegni in Trusted Remediator

Tieni traccia delle tue riparazioni in Trusted Remediator

Dopo aver aggiornato la configurazione a livello di account, Trusted Remediator crea per ogni correzione. OpsItems Trusted Remediator esegue il documento SSM per la riparazione automatica in base al programma di riparazione. OpsItems Per istruzioni su come visualizzare tutte le riparazioni OpsItems dalla OpsCenter console Systems Manager, vedereTieni traccia delle riparazioni in Trusted Remediator.

Esegui riparazioni manuali in Trusted Remediator

Puoi correggere manualmente i Trusted Advisor controlli e i consigli di Compute Optimizer e Security Hub CSPM. Quando si avvia una riparazione manuale, Trusted Remediator crea un'esecuzione manuale. OpsItem È necessario rivedere e avviare il documento di automazione SSM per correggere il. OpsItems Per ulteriori informazioni, consulta Esegui riparazioni manuali in Trusted Remediator.

Raccomandazioni di Compute Optimizer supportate da Trusted Remediator

La tabella seguente elenca i consigli supportati da Compute Optimizer, i documenti di automazione SSM, i parametri preconfigurati e il risultato previsto dei documenti di automazione. Esamina il risultato previsto per aiutarti a comprendere i possibili rischi in base ai requisiti aziendali prima di abilitare un documento di automazione SSM per la correzione degli assegni.

Assicurati che la regola di configurazione corrispondente per ogni controllo di Compute Optimizer sia presente per i controlli supportati per i quali desideri abilitare la correzione. Per ulteriori informazioni, consulta Optare per i controlli. AWS Compute Optimizer Trusted Advisor

Opzione di ottimizzazione	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Corretto dimensionamento		
Consigli sulle istanze Amazon EC2	AWSManagedServices-TrustedRemediatorResizeInstanceByComputeOptimizerRecommendation Tipo di istanza Amazon EC2 aggiornato in base alle raccomand azioni di Compute Optimizer. Le opzioni più ottimali vengono scelte mantenendo gli stessi parametri della piattaforma (architettura, hyperviso r, interfaccia di rete, tipo di virtualiz zazione e così via), se l'opzione esiste.	• MinimumDaysSinceLastChange: Il parametro per specificare il numero minimo di giorni dall'ulti ma modifica del tipo di istanza. L'impostazione di default è 7 giorni. Nessun vincolo • Crea AMIBefore ridimensi onamento: per creare l'AMI dell'ista nza come backup prima del ridimensionamento, imposta su «true». Per non creare un backup, imposta su «false». Il valore predefinito è "true". Nessun vincolo
Raccomand azioni sui volumi di Amazon EBS	AWSManagedServices-ModifyEBSVolume Il volume Amazon EBS viene modificato in base alle raccomand azioni di Compute Optimizer. La modifica può includere il tipo di volume, la dimensione, gli IOPS, la generazione del volume (gp2, gp3 ecc.).	• CreateSnapshot: per creare un'istantanea prima di modificar e il volume, imposta su «true». Per non creare un'istantanea, imposta su «false». L'impostazione predefinita è «true». Nessun vincolo • VolumeType: Il tipo di volume desiderato. Se non viene specifica to alcun tipo, viene mantenuto il tipo esistente.

Opzione di ottimizzazione	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
		Nessun vincolo • VolumeSize: la dimensione desiderata del volume, in GiB. La dimensione del volume di destinazione deve essere maggiore o uguale alla dimensione esistente del volume. Se non viene specificata alcuna dimensione, viene mantenuta la dimensione esistente. Nessun vincolo • Iops: il numero richiesto di I/O operazioni al secondo (IOPS). Questo parametro è valido solo per i volumi io1, io2 e gp3. Nessun vincolo • Throughput: la velocità effettiva necessaria per il provisioning di un volume, con un massimo di 1000 MiB/s. Questo parametro è valido solo per i volumi gp3. Nessun vincolo • RemediateStackDrift: Per avviare la correzione della deriva, se una deriva è causata dalla modifica del volume, imposta su «true». Per non tentare di correggere la deriva, imposta su «false». Il valore predefinito è "true".

Opzione di ottimizzazione	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
		Nessun vincolo
Raccomand azioni sulla funzione Lambda	AWSManagedServices-TrustedR emediatorOptimizeLambdaMemory AWS Lambda memoria delle funzioni ottimizzata secondo le raccomand azioni di Compute Optimizer.	RecommendedMemorySize : dimensione della memoria personali zzata, se diversa dalle opzioni consigliate. Nessun vincolo
Risorse inattive		
Volume Amazon EBS inattivo	AWSManagedServices-DeleteUn usedEBSVolume Il volume Amazon EBS non collegato verrà eliminato.	• CreateSnapshot: per creare un'istantanea prima di eliminare il volume, imposta su «true». Per non creare un'istantanea, imposta su «false». L'impostazione predefinita è «true». Nessun vincolo • MinimumUnattachedDays: minimo giorni non collegati del volume Amazon EBS da eliminare, fino a 62 giorni. L'impostazione predefini ta è 7. Nessun vincolo

Opzione di ottimizzazione	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Istanza Amazon EC2 inattiva	AWSManagedServices-StopECIstanza 2 L'istanza Amazon EC2 inattiva verrà interrotta.	ForceStopWithInstanceStore: Per forzare l'interruzione delle istanze che utilizzano instance store, imposta su «true». Per non forzare l'arresto, imposta su «false». Il valore predefinito 'false' impedisce l'arresto dell'istanza. Nessun vincolo
Istanza Amazon RDS inattiva	AWSManagedServices-StopIdleRDSInstance Interrompi un'istanza Amazon RDS inattiva. I motori supportati sono: MariadB, Microsoft SQL Server, MySQL, Oracle, PostgreSQL. Questo documento non si applica ad Aurora MySQL e Aurora PostgreSQL. L'istanza verrà interrotta per 7 giorni e riavviata automaticamente.	Non sono consentiti parametri preconfigurati. Nessun vincolo

Trusted Advisor controlli supportati da Trusted Remediator

La tabella seguente elenca i Trusted Advisor controlli supportati, i documenti di automazione SSM, i parametri preconfigurati e il risultato previsto dei documenti di automazione. Esamina il risultato previsto per aiutarti a comprendere i possibili rischi in base ai requisiti aziendali prima di abilitare un documento di automazione SSM per la correzione degli assegni.

Assicurati che la regola di configurazione corrispondente per ogni Trusted Advisor controllo sia presente per i controlli supportati per i quali desideri abilitare la correzione. Per ulteriori informazioni, consulta View AWS Trusted Advisor checks powered by. AWS Config Se un controllo ha AWS Security Hub CSPM controlli corrispondenti, assicurati che il controllo CSPM Security Hub sia abilitato. Per ulteriori informazioni, vedere Abilitazione dei controlli in Security Hub CSPM. Per

informazioni sulla gestione dei parametri preconfigurati, vedere Configurare la correzione dei controlli di Trusted Advisor in Trusted Remediator.

Trusted Advisor controlli di ottimizzazione dei costi supportati da Trusted Remediator

Controlla ID e nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Z4 AUBRNSmz Indirizzi IP elastici non associati	AWSManagedServices-TrustedRemediatorReleaseElasticIP Rilascia un indirizzo IP elastico che non è associato a nessuna risorsa.	Non sono consentiti parametri preconfigurati. Nessun vincolo
c18d2gz150 - Istanze Amazon EC2 interrotte	AWSManagedServices-TerminateEC2 InstanceStoppedForPeriodOfTime - Le istanze Amazon EC2 interrotte per un certo numero di giorni vengono terminate.	• Crea AMIBefore terminazione: per creare l'AMI dell'istanza come backup prima di terminare l'istanza Amazon EC2, scegli. `true` Per non creare un backup prima della chiusura, scegli. `false` Il valore predefinito è `true`. • AllowedDays: il numero di giorni in cui l'istanza si trova nello stato di arresto prima che venga terminata. Il valore predefinito è 30. Nessun vincolo
c18d2gz128 Repository di Amazon ECR senza policy del ciclo di vita configurata	AWSManagedServices-TrustedRemediatorPutECRLifecyclePolicy Crea una politica del ciclo di vita per il repository specificato se non esiste già una politica del ciclo di vita.	ImageAgeLimit: il limite di età massimo in giorni (1-365) per «qualsiasi» immagine nell'archivio Amazon ECR. Nessun vincolo
DAvU99Dc4C	AWSManagedServices-DeleteUnusedEBSVolume	• CreateSnapshot: se impostato `sutrue`, l'automazione crea uno

Controlla ID e nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Volumi Amazon EBS sottoutil izzati	Elimina i volumi Amazon EBS sottoutilizzati se i volumi non sono collegati negli ultimi 7 giorni. Per impostazione predefinita, viene creata una snapshot di Amazon EBS.	snapshot del volume Amazon EBS prima che venga eliminato . L'impostazione predefinita è `true`. I valori validi sono `true` e `false` (distinzione tra maiuscole e minuscole). • MinimumUnattachedDays: minimo giorni non allegati del volume EBS da eliminare, fino a 62 giorni. Se impostato su`0`, il documento SSM non verifica il periodo non allegato ed elimina il volume se il volume non è attualmente allegato. Il valore predefinito è. 7 Nessun vincolo

Controlla ID e nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
ciao M8 LMh88u Bilanciatori del carico inattivi	AWSManagedServices-DeleteIdleClassicLoadBalancer Elimina un Classic Load Balancer inattivo se è inutilizzato e non è registrata alcuna istanza.	IdleLoadBalancerDays: Il numero di giorni in cui il Classic Load Balancer ha 0 connessioni richieste prima di considerarlo inattivo. L'impostazione predefinita è sette giorni. Se l'esecuzione automatica è abilitata , l'automazione elimina i Classic Load Balancer inattivi se non ci sono istanze di back-end attive. Per tutti i Classic Load Balancer inattivi che dispongono di istanze di back-end attive, ma non dispongono di istanze di back-end sane, la riparazione automatica non viene utilizzata e viene creata la riparazione manuale. OpsItems
TI39 Half U8 Istanze database Amazon RDS inattive	AWSManagedServices-StopIdleRDSInstance L'istanza database di Amazon RDS che è rimasta inattiva negli ultimi sette giorni viene interrotta.	Non sono consentiti parametri preconfigurati. Nessun vincolo

Controlla ID e nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
COr6dfpM05 AWS Lambda funzioni sovradimensionate per le dimensioni della memoria	AWSManagedServices-ResizeLambdaMemory AWS Lambda la dimensione della memoria della funzione viene ridimensionata alla dimensione di memoria consigliata fornita da. Trusted Advisor	RecommendedMemorySize: l'allocazione di memoria consigliata per la funzione Lambda. L'intervallo di valori è compreso tra 128 e 10240. Se la dimensione della funzione Lambda è stata modificata prima dell'esecuzione dell'automazione, le impostazioni potrebbero essere sovrascritte da questa automazione con il valore consigliato da. Trusted Advisor
QCh7DWoux1 Istanze Amazon EC2 con utilizzo ridotto	AWSManagedServices-StopEC2Instance (documento SSM predefinito per la modalità di esecuzione automatica e manuale). Le istanze Amazon EC2 con basso utilizzo vengono interrotte.	ForceStopWithInstanceStore: impostato su per `true` forzare l'arresto delle istanze utilizzando instance store. In caso contrario, imposta il valore su `false`. Il valore predefinito di `false` impedisce l'arresto dell'istanza. I valori validi sono true o false (distinzione tra maiuscole e minuscole). Nessun vincolo

Controlla ID e nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
QCH7DWoux1 Istanze Amazon EC2 con utilizzo ridotto	AWSManagedServices-ResizeInstanceByOneLevel L'istanza Amazon EC2 viene ridimensionata di un tipo di istanza nello stesso tipo di famiglia di istanze. L'istanza viene interrotta e avviata durante l'operazione di ridimensionamento e riportata allo stato iniziale al termine dell'esecuzione del documento SSM. Questa automazione non supporta il ridimensionamento delle istanze che si trovano in un gruppo di Auto Scaling.	• MinimumDaysSinceLastChange: numero minimo di giorni dall'ultima modifica del tipo di istanza. Se il tipo di istanza è stato modificato entro un periodo di tempo specificato, il tipo di istanza non viene modificato. `0`Utilizzatelo per saltare questa convalida. Il valore predefinito è 7. • Crea AMIBefore ridimensionamento: per creare l'AMI dell'istanza come backup prima del ridimensionamento, scegli. `true` Per non creare un backup, scegli. `false` Il valore predefinito è `false`. I valori validi sono `true` e `false` (distinzione tra maiuscole e minuscole). • ResizeIfStopped: Per procedere con la modifica delle dimensioni dell'istanza, anche se l'istanza è in uno stato interrotto, scegliete . `true` Per non ridimensionare automaticamente l'istanza se si trova in uno stato interrotto, sceglietefalse. I valori validi sono `true` e `false` (distinzione tra maiuscole e minuscole). Nessun vincolo

Controlla ID e nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
QCH7DWoux1 Istanze Amazon EC2 con utilizzo ridotto	AWSManagedServices-TerminateInstance Le istanze Amazon EC2 a basso utilizzo vengono terminate se non fanno parte di un gruppo di Auto Scaling e la protezione dalla terminazione non è abilitata. Per impostazione predefinita, viene creata un'AMI.	Crea AMIBefore terminazione: imposta questa opzione su `true` o per `false` creare un'AMI di istanza come backup prima di terminare l'istanza EC2. Il valore predefinito è `true`. I valori validi sono `true` e `false` (con distinzione tra maiuscole e minuscole). Nessun vincolo
G31sq1e9u Cluster Amazon Redshift sottoutilizzati	AWSManagedServices-PauseRedshiftCluster Il cluster Amazon Redshift è in pausa.	Non sono consentiti parametri preconfigurati. Nessun vincolo
c1cj39rr6v Configurazione di interruzione del caricamento multiparte incompleta di Amazon S3	AWSManagedServices-TrustedRemediatorEnableS3AbortIncompleteMultipartUpload Il bucket Amazon S3 è configurato con una regola del ciclo di vita per interrompere i caricamenti in più parti che rimangono incompleti dopo determinati giorni.	DaysAfterInitiation: il numero di giorni dopo i quali Amazon S3 interrompe un caricamento multiparte incompleto. L'impostazione predefinita è 7 giorni. Nessun vincolo
c1z7kmr00n Raccomandazioni per l'ottimizzazione dei costi di Amazon EC2 per le istanze	Utilizza i consigli sulle istanze Amazon EC2 e l'istanza Amazon EC2 inattiva di. Raccomandazioni di Compute Optimizer supportate da Trusted Remediator	Non sono consentiti parametri preconfigurati. Nessun vincolo

Controlla ID e nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
c1z7kmr02n Raccomandazioni per l'ottimizzazione dei costi di Amazon EBS per i volumi	Utilizza i consigli sui volumi Amazon EBS e il volume Amazon EBS inattivo di. Raccomandazioni di Compute Optimizer supportate da Trusted Remediator	Non sono consentiti parametri preconfigurati. Nessun vincolo
c1z7kmr03n Consigli per l'ottimizzazione dei costi di Amazon RDS per le istanze DB	Usa l'istanza Amazon RDS inattiva di. Raccomandazioni di Compute Optimizer supportate da Trusted Remediator	Non sono consentiti parametri preconfigurati. Nessun vincolo
c1z7kmr05n AWS Lambda raccomandazioni per l'ottimizzazione dei costi per le funzioni	Utilizza i consigli sulla funzione Lambda di. Raccomandazioni di Compute Optimizer supportate da Trusted Remediator	Non sono consentiti parametri preconfigurati. Nessun vincolo

Trusted Advisor controlli di sicurezza supportati da Trusted Remediator

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
12Fnkpl8Y5 Exposed Access Keys	AWSManagedServices-TrustedRemediatorDeactivateIAMAccessKey La chiave di accesso IAM esposta è disattivata.	Non sono consentiti parametri preconfigurati.

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
		Le applicazioni configurate con una chiave di accesso IAM esposta non possono autenticarsi.
Hs4Ma3G127 - API Gateway REST WebSocket e la registrazione dell'esecuzione dell'API devono essere abilitati Controllo corrispondente AWS Security Hub CSPM APIGateway: 1.	AWSManagedServices-TrustedRemediatorEnableAPIGateWayExecutionLogging La registrazione dell'esecuzione è abilitata nella fase API.	LogLevel: Livello di registrazione per abilitare la registrazione dell'esecuzione, `ERROR` - La registrazione è abilitata solo per gli errori. `INFO` - La registrazione è abilitata per tutti gli eventi. Devi concedere ad API Gateway l'autorizzazione a leggere e scrivere i log del tuo account CloudWatch per abilitare il log di esecuzione. Per maggiori dettagli, consulta CloudWatch Configurare la registrazione per REST APIs in API Gateway.
Hs4Ma3G129 - Le fasi API REST API Gateway dovrebbero avere la traccia abilitata AWS X-Ray Controllo corrispondente AWS Security Hub CSPM APIGateway: 3.	AWSManagedServices-EnableApiGateWayXRayTracing Il tracciamento X-Ray è abilitato nella fase API.	Non sono consentiti parametri preconfigurati. Nessun vincolo

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Hs4Ma3G202 - I dati della cache dell'API REST API Gateway devono essere crittografati a riposo Controllo APIGatewaycorrispondente AWS Security Hub CSPM: 5.	AWSManagedServices-EnableAPIGatewayCacheEncryption Abilita la crittografia a riposo per i dati della cache dell'API REST di API Gateway se la fase API REST di API Gateway ha la cache abilitata.	Non sono consentiti parametri preconfigurati. Nessun vincolo
Hs4Ma3G177 - AWS Security Hub CSPM Controllo corrispondente: i gruppi di scalabilità automatica associati a un sistema di bilanciamento del carico devono utilizzare i controlli dello stato del bilanciamento del carico .1 AutoScaling	AWSManagedServices-TrustedRemediatorEnableAutoScalingGroupELBHealthCheck I controlli dello stato di Elastic Load Balancing sono abilitati per il gruppo Auto Scaling.	HealthCheckGracePeriod: la quantità di tempo, in secondi, che Auto Scaling attende prima di verificare lo stato di integrità di un'istanza Amazon Elastic Compute Cloud entrata in servizio. L'attivazione dei controlli di integrità di Elastic Load Balancing potrebbe comportare la sostituzione di un'istanza in esecuzione se uno dei sistemi di bilanciamento del carico Elastic Load Balancing collegati al gruppo Auto Scaling la segnala come non integra. Per ulteriori informazioni, consulta Collegare un sistema di bilanciamento del carico Elastic Load Balancing al gruppo Auto Scaling

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Hs4Ma3G245: gli CloudFormation stack devono essere integrati con Amazon Simple Notification Service Controllo corrispondente AWS Security Hub CSPM : 1. CloudFormation	AWSManagedServices-EnableCFNStackNotification Associa uno CloudFormation stack a un argomento di Amazon SNS per la notifica.	NotificaARNs: gli argomenti ARNs di Amazon SNS da associare a stack selezionati CloudFormation . Per abilitare la riparazione automatica, è necessario fornire il parametro `NotificationARNs` preconfigurato.

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Hs4Ma3G210: le distribuzioni devono avere la registrazione abilitata CloudFront Controllo corrispondente AWS Security Hub CSPM : CloudFront2.	AWSManagedServices-EnableCloudFrontDistributionLogging La registrazione è abilitata per le CloudFront distribuzioni Amazon.	• BucketName: il nome del bucket Amazon S3 in cui desideri archiviare i log di accesso. • S3KeyPrefix: il prefisso per la posizione nel bucket S3 per i log di distribuzione di Amazon. CloudFront • IncludeCookies: Indica se includere i cookie nei log di accesso. Per abilitare la riparazione automatica, è necessario fornire i seguenti parametri preconfigurati: • BucketName • S3KeyPrefix • IncludeCookies Per informazioni su questi vincoli di correzione, vedi Come posso attivare la registrazione per la mia distribuzione? CloudFront

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Hs4Ma3G109: la convalida del file di registro deve essere abilitata CloudTrail Controllo corrispondente AWS Security Hub CSPM : CloudTrail.4	AWSManagedServices-TrustedRemediatorEnableCloudTrailLogValidation Abilita la convalida del registro delle CloudTrail tracce.	Non sono consentiti parametri preconfigurati. Nessun vincolo
Hs4Ma3G108: i CloudTrail trail devono essere integrati con Amazon Logs CloudWatch Controllo corrispondente AWS Security Hub CSPM CloudTrail: 5.	AWSManagedServices-IntegrateCloudTrailWithCloudWatch AWS CloudTrail è integrato con CloudWatch Logs.	• CloudWatchLogsLogGroupName: nome del gruppo di CloudWatch log Logs a cui vengono CloudTrail consegnati i log. Devi utilizzare un gruppo di log esistente nel tuo account. • CloudWatchLogsRoleName: nome del ruolo IAM che l'endpoint CloudWatch Logs deve assumere per scrivere nel gruppo di log di un utente. Devi utilizzare un ruolo esistente nel tuo account. Per abilitare la riparazione automatica, è necessario fornire i seguenti parametri preconfigurati: • CloudWatchLogsLogGroupName • CloudWatchLogsRoleName

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Hs4Ma3G217: gli ambienti di progetto devono avere una configurazione di registrazione CodeBuild AWS Controllo corrispondente AWS Security Hub CSPM CodeBuild: 4.	AWSManagedServices-TrustedRemediatorEnableCodeBuildLoggingConfig Abilita la registrazione del progetto. CodeBuild	Non sono consentiti parametri preconfigurati. Nessun vincolo
Hs4Ma3G306 - I cluster Neptune DB devono avere la protezione da eliminazione abilitata AWS Security Hub CSPM Controllo corrispondente: DocumentDB.3	AWSManagedServices-TrustedRemediatorDisablePublicAccessOnDocumentDBSnapshot Rimuove l'accesso pubblico dallo snapshot manuale del cluster di Amazon DocumentDB.	Non sono consentiti parametri preconfigurati. Nessun vincolo

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Hs4Ma3G308 - I cluster Amazon DocumentDB devono avere la protezione da eliminazione abilitata AWS Security Hub CSPM Controllo corrispondente: DocumentDB.5	AWSManagedServices-TrustedRemediatorEnableDocumentDBClusterDeletionProtection Abilita la protezione da eliminazione per il cluster Amazon DocumentDB.	Non sono consentiti parametri preconfigurati. Nessun vincolo
Hs4Ma3G323 - Le tabelle DynamoDB devono avere la protezione da eliminazione abilitata AWS Security Hub CSPM Controllo corrispondente: DynamoDB.6	AWSManagedServices-TrustedRemediatorEnableDynamoDBTableDeletionProtection Abilita la protezione dall'eliminazione per le tabelle DynamoDB non AMS.	Non sono consentiti parametri preconfigurati. Nessun vincolo
EPS02jt06w - Istantanee pubbliche di Amazon EBS	AWSManagedServices-TrustedRemediatorDisablePublicAccessOnEBSSnapshot L'accesso pubblico per lo snapshot di Amazon EBS è disabilitato.	Non sono consentiti parametri preconfigurati. Nessun vincolo

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Hs4Ma3G118 - I gruppi di sicurezza predefiniti VPC non dovrebbero consentire il traffico in entrata o in uscita Controllo corrispondente AWS Security Hub CSPM : EC2.2	AWSManagedServices-TrustedRemediatorRemoveAllRulesFromDefaultSG Tutte le regole di ingresso e uscita nel gruppo di sicurezza predefinito vengono rimosse.	Non sono consentiti parametri preconfigurati. Nessun vincolo
Hs4Ma3G117 - I volumi EBS collegati devono essere crittografati a riposo Controllo corrispondente AWS Security Hub CSPM : EC2.3	AWSManagedServices-EncryptInstanceVolume Il volume Amazon EBS collegato all'istanza è crittografato.	• KMSKeyId: ID AWS KMS chiave o ARN per crittografare il volume. • DeleteStaleNonEncryptedSnapshotBackups: Un flag che decide se eliminare il backup istantaneo dei vecchi volumi non crittografati. L'istanza viene riavviata come parte della riparazione e il rollback è possibile se `DeleteStaleNonEncryptedSnapshotBackups` è impostato su, il che facilita il ripristino. `false`

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Hs4Ma3G120 - Le istanze EC2 arrestate devono essere rimosse dopo un periodo di tempo specificato Controllo corrispondente AWS Security Hub CSPM : EC2.4	AWSManagedServices-TerminateInstance(documento SSM predefinito per la modalità di esecuzione automatica e manuale) Le istanze Amazon EC2 interrotte per 30 giorni vengono terminate.	Crea terminazione AMIBefore:. Per creare l'AMI dell'istanza come backup prima di terminare l'istanza EC2, scegli. `true` Per non creare un backup prima della chiusura, scegli. `false` Il valore predefinito è `true`. Nessun vincolo
Hs4Ma3G120 - Le istanze EC2 arrestate devono essere rimosse dopo un periodo di tempo specificato Controllo corrispondente AWS Security Hub CSPM : EC2.4	AWSManagedServices-TerminateEC2 InstanceStoppedForPeriodOfTime - Le istanze Amazon EC2 interrotte per il numero di giorni definito in Security Hub (il valore predefinito è 30) vengono terminate.	Crea AMIBefore terminazione: per creare l'AMI dell'istanza come backup prima di terminare l'istanza EC2, scegli. `true` Per non creare un backup prima della chiusura, scegli. `false` Il valore predefinito è `true`. Nessun vincolo

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Hs4Ma3G121 - La crittografia predefinita di EBS deve essere abilitata Controllo corrispondente AWS Security Hub CSPM : EC2.7	AWSManagedServices-EncryptEBSByDefault La crittografia Amazon EBS per impostazione predefinita è abilitata per lo specifico Regione AWS	Non sono consentiti parametri preconfigurati. La crittografia predefinita è un'impostazione specifica della regione. Se lo abiliti per una regione, non puoi disabilitarlo per singoli volumi o istantanee in quella regione.
Hs4Ma3G124 - Le istanze Amazon EC2 devono utilizzare Instance Metadata Service versione 2 () IMDSv2 Controllo corrispondente AWS Security Hub CSPM : EC2.8	AWSManagedServices-TrustedRemediatorAbilita istanza EC2 IMDSv2 Le istanze Amazon EC2 utilizzano Instance Metadata Service versione 2 (). IMDSv2	• IMDSv1MetricCheckPeriod: Il numero di giorni (`42-455`) in cui analizzare i parametri di utilizzo di IMDSv1. CloudWatch Se l'istanza Amazon EC2 è stata creata entro il periodo di tempo specificato, l'analisi inizia dalla data di creazione dell'istanza. • HttpPutResponseHopLimit: Il numero massimo di hop di rete consentiti per il token di metadati dell'istanza. Questo valore può essere configurato tra 1 e 2 hops. Un limite hop 1 limita l'accesso tramite token ai processi in esecuzione direttamente sull'istanza, mentre un limite hop 2 consente l'accesso dai contenitori in esecuzione sull'istanza. Nessun vincolo

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Hs4Ma3G207 - Le sottoreti EC2 non devono assegnare automaticamente indirizzi IP pubblici Controllo corrispondente AWS Security Hub CSPM : EC2.15	AWSManagedServices-UpdateAutoAssignPublicIpv4 indirizzi Le sottoreti VPC sono configurate per non assegnare automaticamente indirizzi IP pubblici.	Non sono consentiti parametri preconfigurati. Nessun vincolo
Hs4Ma3G209 - Gli elenchi di controllo degli accessi alla rete non utilizzati vengono rimossi Controllo corrispondente AWS Security Hub CSPM : EC2.16	AWSManagedServices-DeleteUnusedNACL Eliminare l'ACL di rete non utilizzato	Non sono consentiti parametri preconfigurati. Nessun vincolo

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Hs4Ma3G215 - I gruppi di sicurezza Amazon EC2 non utilizzati devono essere rimossi Controllo corrispondente AWS Security Hub CSPM : EC2.22	AWSManagedServices-DeleteSecurityGroups Eliminare i gruppi di sicurezza non utilizzati.	Non sono consentiti parametri preconfigurati. Nessun vincolo
Hs4Ma3G247 - Amazon EC2 Transit Gateway non dovrebbe accettare automaticamente le richieste di allegati VPC Controllo corrispondente AWS Security Hub CSPM : EC2.23	AWSManagedServices-TrustedRemediatorDisableTGWAutoVPCAttach- Disattiva l'accettazione automatica delle richieste di allegati VPC per lo specifico Amazon EC2 Transit Gateway non AMS.	Non sono consentiti parametri preconfigurati. Nessun vincolo

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Hs4Ma3G235 - I repository privati ECR dovrebbero avere l'immutabilità dei tag configurata Controllo corrispondente AWS Security Hub CSPM : ECR.2	AWSManagedServices-TrustedRemediatorSetImageTagImmutability Imposta le impostazioni di mutabilità del tag di immagine su IMMUTABLE per il repository specificato.	Non sono consentiti parametri preconfigurati. Nessun vincolo
Hs4Ma3G216 - I repository ECR devono avere almeno una politica del ciclo di vita configurata Controllo corrispondente AWS Security Hub CSPM : ECR.3	AWSManagedServices-PutECRRepositoryLifecyclePolicy L'archivio ECR ha una politica del ciclo di vita configurata.	LifecyclePolicyText: Il testo della politica del repository JSON da applicare al repository. Per abilitare la riparazione automatica, è necessario fornire i seguenti parametri preconfigurati: LifecyclePolicyText

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Hs4Ma3G325 - I cluster EKS devono avere la registrazione di controllo abilitata Controllo corrispondente AWS Security Hub CSPM : EKS.8	AWSManagedServices-TrustedRemediatorEnableEKSAuditLog Il registro di controllo è abilitato per il cluster EKS.	Non sono consentiti parametri preconfigurati. Nessun vincolo
Hs4Ma3G183 - Il bilanciamento del carico delle applicazioni deve essere configurato per eliminare le intestazioni HTTP Controllo corrispondente AWS Security Hub CSPM : ELB.4	AWSConfigRemediation-DropInvalidHeadersForALB Application Load Balancer è configurato per campi di intestazione non validi.	Non sono consentiti parametri preconfigurati. Nessun vincolo

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Hs4Ma3G184 - La registrazione di Application Load Balancer e Classic Load Balancers deve essere abilitata Controllo corrispondente AWS Security Hub CSPM : ELB.5	AWSManagedServices-EnableELBLogging (documento SSM predefinito per la modalità di esecuzione automatica e manuale) La registrazione di Application Load Balancer e Classic Load Balancer è abilitata.	• BucketName: il nome del bucket (non l'ARN). Assicurati che la policy del bucket sia configurata correttamente per la registrazione. • S3KeyPrefix: il prefisso per la posizione nel bucket Amazon S3 per i log Elastic Load Balancing. Per abilitare la riparazione automatica, è necessario fornire i seguenti parametri preconfigurati: • BucketName • S3KeyPrefix Il bucket Amazon S3 deve disporre di una policy relativa ai bucket che conceda a Elastic Load Balancing l'autorizzazione a scrivere i log di accesso al bucket.

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Hs4Ma3G184 - La registrazione di Application Load Balancers e Classic Load Balancers deve essere abilitata Controllo corrispondente AWS Security Hub CSPM : ELB.5	AWSManagedServices-EnableELBLoggingV2 La registrazione di Application Load Balancer e Classic Load Balancer è abilitata.	• TargetBucketTagKey: il nome del tag (con distinzione tra maiuscole e minuscole) utilizzato per identificare il bucket Amazon S3 di destinazione. Usalo insieme `TargetBucketTagValue` per etichettare il bucket che fungerà da bucket di destinazione per la registrazione degli accessi. • TargetBucketTagValue: il valore del tag (con distinzione tra maiuscole e minuscole) utilizzato per identificare il bucket Amazon S3 di destinazione. Usalo insieme `TargetBucketTagKey` per etichettare il bucket che fungerà da bucket di destinazione per la registrazione degli accessi. • S3BucketPrefix: il prefisso (gerarchia logica) per il bucket Amazon S3. Il prefisso specificato non deve includere la stringa `AWSLogs`. Per ulteriori informazioni, consulta Organizzazione degli oggetti utilizzando i prefissi. Per abilitare la riparazione automatica, è necessario fornire i seguenti parametri preconfigurati: • TargetBucketTagKey • TargetBucketTagValue • S3BucketPrefix

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
		Il bucket Amazon S3 deve disporre di una policy relativa ai bucket che conceda a Elastic Load Balancing l'autorizzazione a scrivere i log di accesso al bucket.
Hs4Ma3G326 - L'impostazione di accesso pubblico a blocchi di Amazon EMR deve essere abilitata AWS Security Hub CSPM Controllo corrispondente: EMR.2	AWSManagedServices-TrustedRemediatorEnableEMRBlockPublicAccess Le impostazioni di accesso pubblico a blocchi di Amazon EMR sono attivate per l'account.	Non sono consentiti parametri preconfigurati. Nessun vincolo
Hs4Ma3G135: le chiavi non devono essere cancellate involontariamente AWS KMS Controllo corrispondente AWS Security Hub CSPM : KMS.3	AWSManagedServices-CancelKeyDeletion AWS KMS l'eliminazione della chiave viene annullata.	Non sono consentiti parametri preconfigurati. Nessun vincolo

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Hs4Ma3G299 - Le istantanee manuali dei cluster di Amazon DocumentDB non devono essere pubbliche AWS Security Hub CSPM Controllo corrispondente: Neptune.4	AWSManagedServices-TrustedRemediatorEnableNeptuneDBClusterDeletionProtection Abilita la protezione da eliminazione per il cluster Amazon Neptune.	Non sono consentiti parametri preconfigurati. Nessun vincolo
Hs4Ma3G319 - I firewall Network Firewall devono avere la protezione da eliminazione abilitata Controllo corrispondente AWS Security Hub CSPM NetworkFirewall: 9.	AWSManagedServices-TrustedRemediatorEnableNetworkFirewallDeletionProtection- Abilita la protezione da eliminazione per AWS Network Firewall.	Non sono consentiti parametri preconfigurati. Nessun vincolo

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Hs4Ma3G223: i domini devono crittografare i dati inviati tra i nodi OpenSearch Controllo corrispondente AWS Security Hub CSPM : OpenSearch.3	AWSManagedServices-EnableOpenSearchNodeToNodeEncryption La crittografia da nodo a nodo è abilitata per il dominio.	Non sono consentiti parametri preconfigurati. Dopo aver abilitato la node-to-node crittografia, non è possibile disabilitare l'impostazione. Invece, scatta un'istantanea manuale del dominio crittografato, crea un altro dominio, migra i dati e quindi elimina il vecchio dominio.
Hs4Ma3G222: la registrazione degli errori del OpenSearch dominio nei registri deve essere abilitata CloudWatch Controllo corrispondente AWS Security Hub CSPM : Opensearch.4	AWSManagedServices-EnableOpenSearchLogging La registrazione degli errori è abilitata per il dominio. OpenSearch	CloudWatchLogGroupArn: L'ARN di un gruppo di log di Amazon CloudWatch Logs. Per abilitare la riparazione automatica, è necessario fornire il seguente parametro preconfigurato:. CloudWatchLogGroupArn La politica CloudWatch delle risorse di Amazon deve essere configurata con le autorizzazioni. Per ulteriori informazioni, consulta la sezione Abilitazione dei log di controllo nella Amazon OpenSearch Service User Guide

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Hs4Ma3G221: i domini devono avere la registrazione di controllo OpenSearch abilitata Controllo corrispondente AWS Security Hub CSPM : Opensearch.5	AWSManagedServices-EnableOpenSearchLogging OpenSearch i domini sono configurati con la registrazione di controllo abilitata.	CloudWatchLogGroupArn: L'ARN del gruppo CloudWatch Logs in cui pubblicare i log. Per abilitare la riparazione automatica, è necessario fornire il seguente parametro preconfigurato: CloudWatchLogGroupArn La politica CloudWatch delle risorse di Amazon deve essere configurata con le autorizzazioni. Per ulteriori informazioni, consulta la sezione Abilitazione dei log di controllo nella Amazon OpenSearch Service User Guide
Hs4Ma3G220 - Le connessioni ai OpenSearch domini devono essere crittografate utilizzando TLS 1.2 Controllo corrispondente AWS Security Hub CSPM : Opensearch.8	AWSManagedServices-EnableOpenSearchEndpointEncryptionTLS1.2 La politica TLS è impostata su `Policy-min-TLS-1-2-2019-07` e sono consentite solo le connessioni crittografate tramite HTTPS (TLS).	Non sono consentiti parametri preconfigurati. Le connessioni ai OpenSearch domini sono necessarie per utilizzare TLS 1.2. La crittografia dei dati in transito può influire sulle prestazioni. Testa le tue applicazioni con questa funzionalità per comprendere il profilo delle prestazioni e l'impatto del TLS.

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Hs4Ma3G194 - Lo snapshot di Amazon RDS deve essere privato Controllo corrispondente AWS Security Hub CSPM : RDS.1	AWSManagedServices-DisablePublicAccessOnRDSSnapshotV2 L'accesso pubblico per lo snapshot di Amazon RDS è disabilitato.	Non sono consentiti parametri preconfigurati. Nessun vincolo
Hs4Ma3G192 - Le istanze DB RDS dovrebbero vietare l'accesso pubblico, come determinato dalla configurazione PubliclyAccessible AWS Controllo corrispondente AWS Security Hub CSPM : RDS.2	AWSManagedServices-TrustedRemediatorDisablePublicAccessOnRDSInstance Disabilita l'accesso pubblico sull'istanza DB RDS.	Non sono consentiti parametri preconfigurati. Nessun vincolo

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Hs4Ma3G189 - Il monitoraggio avanzato è configurato per le istanze DB di Amazon RDS Controllo corrispondente AWS Security Hub CSPM : RDS.6	AWSManagedServices-TrustedRemediatorEnableRDSEnhancedMonitoring Abilita il monitoraggio avanzato per le istanze DB di Amazon RDS	• MonitoringInterval: L'intervallo, in secondi, tra i punti in cui vengono raccolti i parametri di Enhanced Monitoring per l'istanza DB. Gli intervalli validi sono 0, 1, 5, 10, 15, 30 e 60. Per disabilitare la raccolta dei parametri di monitoraggio avanzato, specifica 0. • MonitoringRoleName: il nome del ruolo IAM che consente ad Amazon RDS di inviare parametri di monitoraggio avanzati ad Amazon Logs. CloudWatch Se un ruolo non è specificato, `rds-monitoring-role` viene utilizzato o creato il ruolo predefinito, se non esiste. Se il monitoraggio avanzato è abilitato prima dell'esecuzione dell'automazione, le impostazioni potrebbero essere sovrascritte da questa automazione con i MonitoringRoleName valori MonitoringInterval e configurati nei parametri preconfigurati.

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Hs4Ma3G190 - I cluster Amazon RDS devono avere la protezione da eliminazione abilitata Controllo corrispondente AWS Security Hub CSPM : RDS.7	AWSManagedServices-TrustedRemediatorEnableRDSDeletionProtection La protezione da eliminazione è abilitata per i cluster Amazon RDS.	Non sono consentiti parametri preconfigurati. Nessun vincolo
Hs4Ma3G198 - Le istanze database di Amazon RDS devono avere la protezione da eliminazione abilitata Controllo corrispondente AWS Security Hub CSPM : RDS.8	AWSManagedServices-TrustedRemediatorEnableRDSDeletionProtection La protezione da eliminazione è abilitata per le istanze Amazon RDS.	Non sono consentiti parametri preconfigurati. Nessun vincolo

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Hs4Ma3G199 - Le istanze DB RDS devono pubblicare i log in Logs CloudWatch Controllo corrispondente AWS Security Hub CSPM : RDS.9	AWSManagedServices-TrustedRemediatorEnableRDSLogExports Le esportazioni dei log RDS sono abilitate per l'istanza DB RDS o il cluster RDS DB.	Non sono consentiti parametri preconfigurati. È richiesto il ruolo AWSServiceRoleForRDS collegato al servizio.
Hs4Ma3G160 - L'autenticazione IAM deve essere configurata per le istanze RDS Controllo corrispondente AWS Security Hub CSPM : RDS.10	AWSManagedServices-UpdateRDSIAMDatabaseAuthentication AWS Identity and Access Management l'autenticazione è abilitata per l'istanza RDS.	ApplyImmediately: indica se le modifiche in questa richiesta e le eventuali modifiche in sospeso vengono applicate in modo asincrono il prima possibile. Per applicare immediatamente la modifica, scegli. `true` Per pianificare la modifica per la prossima finestra di manutenzione, scegliete. `false` Nessun vincolo

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Hs4Ma3G161 - L'autenticazione IAM deve essere configurata per i cluster RDS Controllo corrispondente AWS Security Hub CSPM : RDS.12	AWSManagedServices-UpdateRDSIAMDatabaseAuthentication L'autenticazione IAM è abilitata per il cluster RDS.	ApplyImmediately: Indica se le modifiche in questa richiesta e le eventuali modifiche in sospeso vengono applicate in modo asincrono il prima possibile. Per applicare immediatamente la modifica, scegli. `true` Per pianificare la modifica per la prossima finestra di manutenzione, scegliete. `false` Nessun vincolo
Hs4Ma3G162 - Gli aggiornamenti automatici delle versioni minori di RDS devono essere abilitati Controllo corrispondente AWS Security Hub CSPM : RDS.13	AWSManagedServices-UpdateRDSInstanceMinorVersionUpgrade La configurazione automatica di aggiornamento della versione secondaria per Amazon RDS è abilitata.	Non sono consentiti parametri preconfigurati. L'istanza Amazon RDS deve essere nello `available` stato in cui si verifica questa correzione.

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Hs4Ma3G163 - I cluster DB RDS devono essere configurati per copiare i tag nelle istantanee Controllo corrispondente AWS Security Hub CSPM : RDS.16	AWSManagedServices-UpdateRDSCopyTagsToSnapshots `CopyTagtosnapshot` l'impostazione per i cluster Amazon RDS è abilitata.	Non sono consentiti parametri preconfigurati. Le istanze di Amazon RDS devono essere disponibili affinché questa correzione avvenga.
Hs4Ma3G164 - Le istanze DB RDS devono essere configurate per copiare i tag nelle istantanee Controllo corrispondente AWS Security Hub CSPM : RDS.17	AWSManagedServices-UpdateRDSCopyTagsToSnapshots `CopyTagsToSnapshot` l'impostazione per Amazon RDS è abilitata.	Non sono consentiti parametri preconfigurati. Le istanze di Amazon RDS devono essere disponibili affinché questa correzione avvenga.
RSS93 HQwa1 Snapshot pubblici di Amazon RDS	AWSManagedServices-DisablePublicAccessOnRDSSnapshotV2 L'accesso pubblico per lo snapshot di Amazon RDS è disabilitato.	Non sono consentiti parametri preconfigurati. Nessun vincolo

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Hs4Ma3G103 - I cluster Amazon Redshift dovrebbero vietare l'accesso pubblico AWS Security Hub CSPM Controllo corrispondente: Redshift.1	AWSManagedServices-DisablePublicAccessOnRedshiftCluster L'accesso pubblico sul cluster Amazon Redshift è disabilitato.	Non sono consentiti parametri preconfigurati. La disabilitazione dell'accesso pubblico blocca tutti i client provenienti da Internet. Inoltre, il cluster Amazon Redshift rimane in stato di modifica per alcuni minuti, mentre la riparazione disabilita l'accesso pubblico al cluster.
Hs4Ma3G106 - I cluster Amazon Redshift devono avere la registrazione di controllo abilitata AWS Security Hub CSPM Controllo corrispondente: Redshift.4	AWSManagedServices-TrustedRemediatorEnableRedshiftClusterAuditLogging La registrazione di audit è abilitata sul cluster Amazon Redshift durante la finestra di manutenzione.	Non sono consentiti parametri preconfigurati. Per abilitare la riparazione automatica, è necessario fornire i seguenti parametri preconfigurati. BucketName: Il secchio deve essere nello stesso. Regione AWS Il cluster deve disporre dei permessi di lettura per bucket e put object. Se la registrazione del cluster Redshift è abilitata prima dell'esecuzione dell'automazione, le impostazioni di registrazione potrebbero essere sovrascritte da questa automazione con `S3KeyPrefix` i valori `BucketName` e configurati nei parametri preconfigurati.

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Hs4Ma3G105 - Amazon Redshift dovrebbe avere gli aggiornamenti automatici alle versioni principal i abilitati AWS Security Hub CSPM Controllo corrispondente: Redshift.6	AWSManagedServices-EnableRedshiftClusterVersionAutoUpgrade-Gli aggiornamenti delle versioni principali vengono applicati automaticamente al cluster durante la finestra di manutenzione. Non ci sono tempi di inattività immediati per il cluster Amazon Redshift, ma il cluster Amazon Redshift potrebbe subire dei tempi di inattività durante la finestra di manutenzione se passa a una versione principale.	Non sono consentiti parametri preconfigurati. Nessun vincolo
Hs4Ma3G104 - I cluster Amazon Redshift devono utilizzare un routing VPC avanzato AWS Security Hub CSPM Controllo corrispondente: Redshift.7	AWSManagedServices-TrustedRemediatorEnableRedshiftClusterEnhancedVPCRouting Il routing VPC avanzato è abilitato per i cluster Amazon Redshift.	Non sono consentiti parametri preconfigurati. Nessun vincolo

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Hs4Ma3G173 - L'impostazione S3 Block Public Access deve essere abilitata a livello di bucket Controllo corrispondente AWS Security Hub CSPM : S3.8	AWSManagedServices-TrustedRemediatorBlockS3BucketPublicAccess I blocchi di accesso pubblico a livello di bucket vengono applicati per il bucket Amazon S3.	Non sono consentiti parametri preconfigurati. Questa correzione potrebbe influire sulla disponibilità degli oggetti S3. Per informazioni su come Amazon S3 valuta l'accesso, consulta Bloccare l'accesso pubblico allo storage Amazon S3.

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Hs4Ma3G230 - La registrazione degli accessi al server bucket S3 deve essere abilitata Controllo corrispondente AWS Security Hub CSPM : S3.9	AWSManagedServices-EnableBucketAccessLogging(documento SSM predefinito per la modalità di esecuzione automatica e manuale) La registrazione degli accessi ai server Amazon S3 è abilitata.	• TargetBucket: il nome del bucket S3 per archiviare i log di accesso al server. • TargetObjectKeyFormat: formato chiave Amazon S3 per oggetti di log (i valori fanno distinzione tra maiuscole e minuscole). Per utilizzare il formato semplice per le chiavi S3 per gli oggetti di registro, scegli. `SimplePrefix` Per utilizzare la chiave S3 partizionata per gli oggetti di registro e utilizzarla EventTime per il prefisso partizionato, scegli. `PartitionedPrefixEventTime` Per utilizzare la chiave S3 partizionata per gli oggetti di registro e utilizzarla per il prefisso partizionato, scegliete . DeliveryTime `PartitionedPrefixDeliveryTime` I valori validi sono `SimplePrefix` , `PartitionedPrefixEventTime` e `PartitionedPrefixDeliveryTime` . Per abilitare la riparazione automatica, è necessario fornire il seguente parametro preconfigurato:. TargetBucket Il bucket di destinazione deve trovarsi nello stesso Regione AWS e

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
		Account AWS nel bucket di origine, con le autorizzazioni corrette per la consegna dei log. Per ulteriori informazioni, consulta Abilitazione della registrazione degli accessi al server Amazon S3.

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Hs4Ma3G230 — La registrazione degli accessi al server bucket S3 deve essere abilitata Controllo corrispondente AWS Security Hub CSPM : S3.9	AWSManagedServices-TrustedRemediatorEnableBucketAccessLoggingV2 - La registrazione dei bucket di Amazon S3 è abilitata.	• TargetBucketTagKey: Il nome del tag (con distinzione tra maiuscole e minuscole) per identificare il bucket di destinazione. Utilizzat elo TargetBucketTagValueper etichettare il bucket da utilizzare come bucket di destinazione per la registrazione degli accessi. • TargetBucketTagValue: Il valore del tag (con distinzione tra maiuscole e minuscole) per identificare il bucket di destinazi one, usalo e TargetBucketTagKey per etichettare il bucket da utilizzar e come bucket di destinazione per la registrazione degli accessi. • TargetObjectKeyFormat: Formato chiave Amazon S3 per oggetti di log (i valori fanno distinzione tra maiuscole e minuscole): per utilizzare il formato semplice per le chiavi S3 per gli oggetti di log, scegli. SimplePrefix Per utilizzar e la chiave S3 partizionata per gli oggetti di log e EventTime utilizzarla per il prefisso partizion ato, scegli. PartitionedPrefixE ventTime Per utilizzare la chiave S3 partizionata per gli oggetti di registro e utilizzarla per il prefisso partizionato, scegliete. DeliveryT ime PartitionedPrefixDeliveryTi

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
		me Il valore predefinito è Partition edPrefixEventTime. Per abilitare la riparazione automatic a, è necessario fornire i seguenti parametri: TargetBucketTagKeye TargetBucketTagValue. Il bucket di destinazione deve trovarsi nello stesso Regione AWS e Account AWS nel bucket di origine, con le autorizzazioni corrette per la consegna dei log. Per ulteriori informazioni, consulta Abilitazione della registrazione degli accessi al server Amazon S3.
Pfx0 RwqBli Autorizzazioni Bucket Amazon S3	AWSManagedServices-TrustedRemediatorBlockS3BucketPublicAccess Blocca l'accesso pubblico	Non sono consentiti parametri preconfigurati. Questo controllo è costituito da più criteri di avviso. Questa automazione risolve i problemi di accesso pubblico. La risoluzione di altri problemi di configurazione segnalati da Trusted Advisor non è supportata. Questa riparazione supporta la riparazione dei bucket S3 Servizio AWS creati (ad esempio, cf-templates-000000000000).

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Hs4Ma3G272 - Gli utenti non devono avere accesso root alle istanze dei notebook SageMaker Controllo corrispondente AWS Security Hub CSPM SageMaker: 3.	AWSManagedServices-TrustedRemediatorDisableSageMakerNotebookInstanceRootAccess L'accesso root per gli utenti è disabilitato per l'istanza del SageMaker notebook.	Non sono consentiti parametri preconfigurati. Questa riparazione causa un'interruzione se l'istanza del SageMaker notebook si trova nello stato in cui si trova. InService
Hs4Ma3G179 - Gli argomenti SNS devono essere crittografati a riposo utilizzando AWS KMS Controllo corrispondente AWS Security Hub CSPM : SNS.1	AWSManagedServices-EnableSNSEncryptionAtRest L'argomento SNS è configurato con la crittografia lato server.	KmsKeyId: l'ID di una chiave master del cliente AWS gestita (CMK) per Amazon SNS o di una CMK personalizzata da utilizzare per la crittografia lato server (SSE). `alias/aws/sns` L'impostazione predefinita è impostata su. Se viene utilizzata una AWS KMS chiave personalizzata, deve essere configurata con le autorizzazioni corrette. Per ulteriori informazioni, consulta Attivazione della crittografia lato server (SSE) per un argomento Amazon SNS

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Hs4Ma3G158 - I documenti SSM non devono essere pubblici Controllo corrispondente AWS Security Hub CSPM : SSM.4	AWSManagedServices-TrustedRemediatorDisableSSMDocPublicSharing- Disabilita la condivisione pubblica del documento SSM.	Non sono consentiti parametri preconfigurati. Nessun vincolo

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Hs4Ma3G136 - Le code di Amazon SQS devono essere crittografate quando sono inattive Controllo corrispondente AWS Security Hub CSPM : SQS.1	AWSManagedServices-EnableSQSEncryptionAtRest I messaggi in Amazon SQS sono crittografati.	• SqsManagedSseEnabled: impostato per `true` abilitare la crittografia delle code lato server utilizzando chiavi di crittografia di proprietà di Amazon SQS, impostato per `false` abilitare la crittografia delle code lato server utilizzando una chiave. AWS KMS • KMSKeyId: l'ID o l'alias di una chiave master del cliente AWS gestita (CMK) per Amazon SQS o di una CMK personalizzata da utilizzare per la crittografia lato server per la coda. Se non fornito, viene utilizzato. alias/aws/sqs • KmsDataKeyReusePeriodSeconds: il periodo di tempo, in secondi, durante il quale Amazon SQS può riutilizzare una chiave dati per crittografare o decrittografare i messaggi prima di effettuare una nuova chiamata. AWS KMS Numero intero che rappresenta secondi, tra 60 (1 minuto) e 86.400 (24 ore). Questa impostazione viene ignorata se è impostata su. `SqsManagedSseEnabled` `true` ReceiveMessage Le richieste anonime SendMessage e quelle inviate alla coda crittografata vengono rifiutate. Tutte le richieste

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
		alle code con la funzione SSE abilitata devono utilizzare HTTPS e Signature Version 4.

Trusted Advisor controlli di tolleranza agli errori supportati da Trusted Remediator

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
c18d2gz138 Ripristino Amazon DynamoDB Point-in-time	AWSManagedServices-TrustedRemediatorEnableDDBPITR Abilita point-in-time il ripristino per le tabelle DynamoDB.	Non sono consentiti parametri preconfigurati. Nessun vincolo
R365S2qddf Amazon S3 Bucket Versioning	AWSManagedServices-TrustedRemediatorEnableBucketVersioning Il controllo delle versioni del bucket Amazon S3 è abilitato.	Non sono consentiti parametri preconfigurati. Questa correzione non supporta la riparazione dei bucket S3 Servizio AWS creati (ad esempio cf-templates-000000000000).
BueAdJ7nRP Registrazione di Bucket Amazon S3	AWSManagedServices-EnableBucketAccessLogging La registrazione dei bucket Amazon S3 è abilitata.	• TargetBucket: il nome del bucket S3 per archiviare i log di accesso al server. • TargetObjectKeyFormat: formato chiave Amazon S3 per oggetti di log, per utilizzare il formato semplice per le chiavi S3 per gli oggetti di log, scegli. `SimplePrefix` Per utilizzare la chiave Partitioned S3 per gli oggetti di log

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
		e usarla per il prefisso partizionato, EventTime scegli. `PartitionedPrefixEventTime` Per utilizzare la chiave S3 partizionata per gli oggetti di registro e utilizzarla per il prefisso partizionato, scegliete. DeliveryTime `PartitionedPrefixDeliveryTime` Il valore predefinito è `PartitionedPrefixEventTime` . I valori validi sono `SimplePrefix` e (con distinzione tra maiuscole e minuscole). `PartitionedPrefixEventTime` `PartitionedPrefixDeliveryTime` Per abilitare la riparazione automatica, è necessario fornire i seguenti parametri preconfigurati: • TargetBucket Il bucket di destinazione deve trovarsi nello stesso Regione AWS e Account AWS nel bucket di origine, con le autorizzazioni corrette per la consegna dei log. Per ulteriori informazioni, consulta Abilitazione della registrazione degli accessi al server Amazon S3.

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
F2ik5r6dep Amazon RDS Multi-AZ	AWSManagedServices-TrustedRemediatorEnableRDSMultiAZ L'implementazione di più zone di disponibilità è abilitata.	Non sono consentiti parametri preconfigurati. C'è un possibile peggioramento delle prestazioni durante questa modifica.
H7 IgTzj TYb Snapshot Amazon EBS	AWSManagedServices-TrustedRemediatorCreateEBSSnapshot Viene creato Amazon EBSsnapshots .	Non sono consentiti parametri preconfigurati. Nessun vincolo
Top ZvH QPADk Backup RDS	AWSManagedServices-EnableRDSBackupRetention La conservazione dei backup di Amazon RDS è abilitata per il DB.	• BackupRetentionPeriod: Il numero di giorni (1-35) per conservare i backup automatici. • ApplyImmediately: Indica se la modifica della conservazione del backup RDS e le eventuali modifiche in sospeso vengono applicate in modo asincrono il prima possibile. Scegli `true` di applicare la modifica immediata mente o di pianificare la modifica `false` per la finestra di manutenzi one successiva. Se il `ApplyImmediately` parametro è impostato su`true`, le modifiche in sospeso sul db vengono applicate insieme all'impostazione di RDSBackup conservazione.

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
c1qf5bt013 La scalabilità automatica dello storage sulle istanze DB di Amazon RDS è disattivata	AWSManagedServices-TrustedRemediatorEnableRDSInstanceStorageAutoScaling- La scalabilità automatica dello storage è abilitata per le istanze database di Amazon RDS.	• MaxAllocatedStorageIncrease Percentage: La percentuale di aumento della corrente Allocated Storage, per impostare la. MaxAllocatedStorage L'impostazione predefinita è impostata su26. È necessario impostare la soglia massima di archiviazione su almeno il 10% in più rispetto allo spazio di archiviazione attualmente allocato. È consigliabile impostare la soglia massima di archiviazione su almeno il 26% in più. Per maggiori dettagli, consulta Gestire automaticamente la capacità con lo storage autoscaling di Amazon Relational Database Service. Nessun vincolo
7q GXs KIUw Drenaggio della connessione Classic Load Balancer	AWSManagedServices-TrustedRemediatorEnableCLBConnectionDraining Il drenaggio della connessione è abilitato per Classic Load Balancer.	ConnectionDrainingTimeout: Il tempo massimo, in secondi, per mantenere aperte le connessioni esistenti prima di annullare la registrazione delle istanze. L'impostazione predefinita è impostata su secondi. `300` Nessun vincolo

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
c18d2gz106 Amazon EBS non incluso nel piano AWS Backup	AWSManagedServices-TrustedRemediatorAddVolumeToBackupPlan Amazon EBS è incluso nel AWS Backup piano.	Remediation contrassegna il volume Amazon EBS con la seguente coppia di tag. La coppia di tag deve corrispondere ai criteri di selezione delle risorse basati su tag per. AWS Backup • TagKey • TagValue Nessun vincolo
c18d2gz107 Tabella Amazon DynamoDB non inclusa nel piano AWS Backup	AWSManagedServices-TrustedRemediatorAddDynamoDBToBackupPlan Amazon DynamoDB Table è inclusa nel piano. AWS Backup	Remediation contrassegna Amazon DynamoDB con la seguente coppia di tag. La coppia di tag deve corrispondere ai criteri di selezione delle risorse basati su tag per. AWS Backup • TagKey • TagValue Nessun vincolo

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
c18d2gz117 Amazon EFS non incluso nel AWS Backup piano	AWSManagedServices-TrustedRemediatorAddEFSToBackupPlan Amazon EFS è incluso nel AWS Backup piano.	Remediation contrassegna Amazon EFS con la seguente coppia di tag. La coppia di tag deve corrispondere ai criteri di selezione delle risorse basati su tag per. AWS Backup • TagKey • TagValue Nessun vincolo
c18d2gz105 Bilanciamento del carico tra zone di Network Load Balancer	AWSManagedServices-TrustedRemediatorEnableNLBCrossZoneLoadBalancing Il bilanciamento del carico tra zone è abilitato su Network Load Balancer.	Non sono consentiti parametri preconfigurati. Nessun vincolo
c1qf5bt026 Il `synchronous_commit` parametro Amazon RDS è disattivato	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter Il parametro `synchronous_commit` è attivato per Amazon RDS.	Non sono consentiti parametri preconfigurati. Nessun vincolo
c1qf5bt030 Il `innodb_flush_log_at_trx_commit` parametro Amazon RDS non lo è 1	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter Il parametro `innodb_flush_log_at_trx_commit` è impostato su 1 per Amazon RDS.	Non sono consentiti parametri preconfigurati. Nessun vincolo

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
c1qf5bt031 Il `sync_binlog` parametro Amazon RDS è disattivato	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter Il parametro `sync_binlog` è attivato per Amazon RDS.	Non sono consentiti parametri preconfigurati. Nessun vincolo
c1qf5bt036 L'impostazione dei `innodb_default_row_format` parametri Amazon RDS non è sicura	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter Il parametro `innodb_default_row_format` è impostato su `DYNAMIC` per Amazon RDS.	Non sono consentiti parametri preconfigurati. Nessun vincolo
c18d2gz144 Monitoraggio dettagliato di Amazon EC2 non abilitato	AWSManagedServices-TrustedRemediatorEnableEC2InstanceDetailedMonitoring Il monitoraggio dettagliato è abilitato per Amazon EC2.	Non sono consentiti parametri preconfigurati. Nessun vincolo

Trusted Advisor controlli delle prestazioni supportati da Trusted Remediator

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
COr6dfpM06 AWS Lambda funzioni non sufficientemente fornite per	AWSManagedServices-ResizeLambdaMemory Le dimensioni della memoria delle funzioni Lambda vengono ridimensionate alla dimensione di memoria	RecommendedMemorySize: l'allocazione di memoria consigliata per la funzione Lambda. L'intervallo di valori è compreso tra 128 e 10240.

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
quanto riguarda le dimensioni della memoria	consigliata fornita da. Trusted Advisor	Se la dimensione della funzione Lambda viene modificata prima dell'esecuzione dell'automazione, questa automazione potrebbe sovrascrivere le impostazioni con il valore consigliato da. Trusted Advisor

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
ZRxQlPsb6c Istanze Amazon EC2 con utilizzo elevato	AWSManagedServices-ResizeInstanceByOneLevel Le istanze Amazon EC2 vengono ridimensionate di un tipo di istanza in su nello stesso tipo di famiglia di istanze. Le istanze vengono interrotte e avviate durante l'operazione di ridimensionamento e riportate allo stato iniziale al termine dell'esecuzione. Questa automazione non supporta il ridimensionamento delle istanze che si trovano in un gruppo di Auto Scaling.	• MinimumDaysSinceLastChange: Il numero minimo di giorni trascorsi dall'ultima modifica del tipo di istanza. Se il tipo di istanza è stato modificato entro il tempo specificato, il tipo di istanza non viene modificato. `0`Utilizzatelo per saltare questa convalida. Il valore predefinito è 7. • Crea AMIBefore ridimensionamento: per creare l'AMI dell'istanza come backup prima del ridimensionamento, scegli. `true` Per non creare un backup, scegli. `false` Il valore predefinito è `false`. I valori validi sono `true` e `false` (distinzione tra maiuscole e minuscole). • ResizeIfStopped: Per procedere con la modifica delle dimensioni dell'istanza, anche se l'istanza è in uno stato interrotto, scegliete . `true` Per non ridimensionare automaticamente l'istanza se si trova in uno stato interrotto, sceglietefalse. I valori validi sono `true` e `false` (distinzione tra maiuscole e minuscole). Nessun vincolo

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
c1qf5bt021 `innodb_change_buffering` Parametro Amazon RDS che utilizza un valore inferiore a quello ottimale	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter Il valore del `innodb_change_buffering` parametro è impostato su `NONE` per Amazon RDS.	Non sono consentiti parametri preconfigurati. Nessun vincolo
c1qf5bt025 Il `autovacuum` parametro Amazon RDS è disattivato	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter Il parametro `autovacuum` è attivato per Amazon RDS.	Non sono consentiti parametri preconfigurati. Nessun vincolo
c1qf5bt028 Il `enable_indexonlyscan` parametro Amazon RDS è disattivato	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter Il parametro `enable_indexonlyscan` è attivato per Amazon RDS.	Non sono consentiti parametri preconfigurati. Nessun vincolo
c1qf5bt029 Il `enable_indexscan` parametro Amazon RDS è disattivato	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter Il parametro `enable_indexscan` è attivato per Amazon RDS.	Non sono consentiti parametri preconfigurati. Nessun vincolo

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
c1qf5bt032 Il `innodb_stats_persistent` parametro Amazon RDS è disattivato	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter Il parametro `innodb_stats_persistent` è attivato per Amazon RDS.	Non sono consentiti parametri preconfigurati. Nessun vincolo
c1qf5bt037 Il `general_logging` parametro Amazon RDS è attivato	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter Il parametro `general_logging` è disattivato per Amazon RDS.	Non sono consentiti parametri preconfigurati. Nessun vincolo

Trusted Advisor controlli dei limiti di servizio supportati da Trusted Remediator

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
RR0l7Ln7 J9 Indirizzo IP elastico EC2-VPC	AWSManagedServices-UpdateVpcElasticIPQuota È richiesto un nuovo limite per gli indirizzi IP elastici EC2-VPC. Per impostazione predefinita, il limite viene aumentato di 3.	Incremento: il numero per aumentare la quota corrente. Il valore predefinito è 3. Se questa automazione viene eseguita più volte prima che il Trusted Advisor controllo venga aggiornato con lo 0K stato, potrebbe verificarsi un aumento del limite più elevato.

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Km7 J9 QQ0l7 Gateway Internet VPC	AWSManagedServices-IncreaseServiceQuota- È richiesto un nuovo limite per i gateway Internet VPC. Per impostazione predefinita, il limite viene aumentato di tre.	Incremento: il numero per aumentare la quota corrente. Il valore predefinito è 3. Se questa automazione viene eseguita più volte prima che il Trusted Advisor controllo venga aggiornato con lo 0K stato, potrebbe verificarsi un aumento del limite più elevato.
jL7 J9 PP0l7 VPC	AWSManagedServices-IncreaseServiceQuota È richiesto un nuovo limite per il VPC. Per impostazione predefinita, il limite viene aumentato di 3.	Incremento: il numero per aumentare la quota corrente. Il valore predefinito è 3. Se questa automazione viene eseguita più volte prima che il Trusted Advisor controllo venga aggiornato con lo 0K stato, potrebbe verificarsi un aumento del limite più elevato.
fW7 J9 HH0l7 Gruppi Auto Scaling	AWSManagedServices-IncreaseServiceQuota È richiesto un nuovo limite per i gruppi di Auto Scaling. Per impostazi one predefinita, il limite viene aumentato di 3.	Incremento: il numero per aumentare la quota corrente. Il valore predefinito è 3. Se questa automazione viene eseguita più volte prima che il Trusted Advisor controllo venga aggiornato con lo 0K stato, potrebbe verificarsi un aumento del limite più elevato.

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
3 Njm0 DJQO9 Gruppi di opzioni RDS	AWSManagedServices-Increase ServiceQuota È richiesto un nuovo limite per i gruppi di opzioni Amazon RDS. Per impostazione predefinita, il limite viene aumentato di 3.	Incremento: il numero per aumentare la quota corrente. Il valore predefinito è 3. Se questa automazione viene eseguita più volte prima che il Trusted Advisor controllo venga aggiornato con lo 0K stato, potrebbe verificarsi un aumento del limite più elevato.
EM8b3yLRTr Application Load Balancer ELB	AWSManagedServices-Increase ServiceQuota È richiesto un nuovo limite per ELB Application Load Balancers. Per impostazione predefinita, il limite viene aumentato di 3.	Incremento: il numero per aumentare la quota corrente. Il valore predefinito è 3. Se questa automazione viene eseguita più volte prima che il Trusted Advisor controllo venga aggiornato con lo 0K stato, potrebbe verificarsi un aumento del limite più elevato.
8 WiQ K YSt25 Bilanciatori del carico di rete ELB	AWSManagedServices-Increase ServiceQuota È richiesto un nuovo limite per ELB Network Load Balancer. Per impostazione predefinita, il limite viene aumentato di 3.	Incremento: il numero per aumentare la quota corrente. Il valore predefinito è 3. Se questa automazione viene eseguita più volte prima che il Trusted Advisor controllo venga aggiornato con lo 0K stato, potrebbe verificarsi un aumento del limite più elevato.

Trusted Advisor controlli di eccellenza operativa supportati da Trusted Remediator

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
c18d2gz125 Il Gateway Amazon API non registra log di esecuzione	AWSManagedServices-TrustedRemediatorEnableAPIGateWayExecutionLogging La registrazione dell'esecuzione è abilitata nella fase API.	Non sono consentiti parametri preconfigurati. Devi concedere ad API Gateway l'autorizzazione a leggere e scrivere i log del tuo account CloudWatch per abilitare il log di esecuzione. Per maggiori dettagli, consulta CloudWatch Configurare la registrazione per REST APIs in API Gateway.
c18d2gz168 Protezione dall'eliminazione Elastic Load Balancing non abilitata per i sistemi di bilanciamento del carico	AWSManagedServices-TrustedRemediatorEnableELBDeletionProtection- La protezione da eliminazione è attivata per Elastic Load Balancer.	Non sono consentiti parametri preconfigurati. Nessun vincolo
c1qf5bt012 Amazon RDS Performance Insights è disattivato	AWSManagedServices-TrustedRemediatorEnableRDSPerformanceInsights Performance Insights è attivato per Amazon RDS.	• PerformanceInsightsRetentionPeriod: il numero di giorni per conservare i dati di Performance Insights. Valori validi: 7 o mese * 31, dove mese è un numero di mesi compreso tra 1 e 23. Esempi: 93 (3 mesi* 31), 341 (11 mesi* 31), 589 (19 mesi* 31) oppure731. • PerformanceInsightsKMSKeyId: l'ID AWS KMS chiave per la crittografia dei dati di Performan

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
		ce Insights. Se non specifichi un valore per PerformanceInsights KMSKey Id, Amazon RDS utilizza la tua AWS KMS chiave predefini ta. Nessun vincolo

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
c1fd6b96l4 Registri di accesso Amazon S3 abilitati	AWSManagedServices-TrustedRemediatorEnableBucketAccessLoggingV2 La registrazione degli accessi ai bucket Amazon S3 è abilitata.	• TargetBucketTagValue: Il valore del tag (con distinzione tra maiuscole e minuscole) per identificare il bucket di destinazione, utilizzalo e TargetBucketTagKey contrassegna il bucket da utilizzare come bucket di destinazione per la registrazione degli accessi. • TargetObjectKeyFormat: formato chiave Amazon S3 per oggetti di log (i valori fanno distinzione tra maiuscole e minuscole). Per utilizzare il formato semplice per le chiavi S3 per gli oggetti di registro, scegli. `SimplePrefix` Per utilizzare la chiave S3 partizionata per gli oggetti di registro e utilizzarla EventTime per il prefisso partizionato, scegli. `PartitionedPrefixEventTime` Per utilizzare la chiave S3 partizionata per gli oggetti di registro e utilizzarla per il prefisso partizionato, scegliete . DeliveryTime `PartitionedPrefixDeliveryTime` I valori validi sono `SimplePrefix` , `PartitionedPrefixEventTime` e `PartitionedPrefixDeliveryTime` .

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
		Per abilitare la riparazione automatic a, è necessario fornire il seguente parametro preconfigurato: TargetBuc ketTagKeye. TargetBucketTagValue Il bucket di destinazione deve trovarsi nello stesso Regione AWS e Account AWS nel bucket di origine, con le autorizzazioni corrette per la consegna dei log. Per ulteriori informazioni, consulta Abilitazione della registrazione degli accessi al server Amazon S3.

Raccomandazioni CSPM di Security Hub supportate da Trusted Remediator

La tabella seguente elenca i consigli CSPM supportati da Security Hub, i documenti di automazione SSM, i parametri preconfigurati e il risultato previsto dei documenti di automazione. Esamina il risultato previsto per aiutarti a comprendere i possibili rischi in base ai requisiti aziendali prima di abilitare un documento di automazione SSM per la correzione degli assegni.

Assicurati di abilitare Security Hub CSPM per l'account. Per ulteriori informazioni, vedere, Enabling Security Hub CSPM.

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Security-Hub-IAM-22 IAM.22: le credenziali utente IAM non utilizzate per 45	AWSManagedServices-TrustedR emediatorDeactivateIamUserU nusedCredentials	DeleteAccessKeys: Imposta su true per eliminare definitivamente le chiavi di accesso non utilizzate o su false per disattivarle (rendendole inattive ma recuperabili). Nessun vincolo

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
giorni devono essere rimosse.		
Security-hub-IAM-3 IAM.3: le chiavi di accesso degli utenti IAM devono essere ruotate ogni 90 giorni o meno.	AWSManagedServices-TrustedRemediatorRotateIamAccessKeysOlderThan90 giorni	Non sono consentiti parametri preconfigurati. Nessun vincolo
Security-hub-IAM-8 IAM.8: le credenziali utente IAM non utilizzate devono essere rimosse.	AWSManagedServices-TrustedRemediatorDeactivateIamUserUnusedCredentials	DeleteAccessKeys: Imposta su true per eliminare definitivamente le chiavi di accesso non utilizzate o su false per disattivarle (rendendole inattive ma recuperabili). Nessun vincolo
security-hub-networkfirewall-10 NetworkFirewall.10 : I firewall Network Firewall devono avere la protezione da modifica della sottorete abilitata :	AWSManagedServices-TrustedRemediatorEnableNetworkFirewallSubnetChangeProtection	Non sono consentiti parametri preconfigurati. Nessun vincolo

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
security-hub-networkfirewall-2 NetworkFirewall.2: La registrazione del Network Firewall deve essere abilitata.	AWSManagedServices-TrustedRemediatorEnableNetworkFirewallCloudWatchLog	LogGroupName: il nome del gruppo di CloudWatch log a cui inviare i log. LogTypes: i tipi di log da abilitare. I valori validi sono `FLOW`, `ALERT`, `TLS`. Nessun vincolo
security-hub-stepfunctions-1 StepFunctions.1: Le macchine a stati Step Functions dovrebbero avere la registrazione attivata.	AWSManagedServices-TrustedRemediatorEnableStepFunctionsLogging	LogGroupName: il nome del gruppo di CloudWatch log per la registrazione di Step Functions. LoggingLevel: Il livello di registrazione per Step Functions. I valori validi sono `ALL`, `ERROR`, `FATAL`.
security-hub-lambda-7 Lambda.7: le funzioni Lambda devono avere il tracciamento attivo AWS X-Ray abilitato.	AWSManagedServices-TrustedRemediatorEnableLambdaXrayActiveTracing	Non sono consentiti parametri preconfigurati. Nessun vincolo

Configurare Trusted Advisor la correzione degli assegni in Trusted Remediator

Le configurazioni vengono archiviate AWS AppConfig come parte dell'applicazione Trusted Remediator. Ogni categoria di Trusted Advisor controllo ha un profilo di configurazione separato. Per ulteriori informazioni sulle Trusted Advisor categorie, consulta Visualizza le categorie di controllo.

È possibile configurare le riparazioni in base alla risorsa o al controllo. Trusted Advisor È possibile applicare eccezioni utilizzando i tag delle risorse.

> **Note**
>
> La correzione dei Trusted Advisor risultati è attualmente configurata utilizzando AWS AppConfig e questa funzionalità è attualmente completamente supportata. AMS prevede che questo cambierà in futuro. È consigliabile evitare di creare automazioni che dipendono da AWS AppConfig, poiché questo metodo è soggetto a modifiche. Tieni presente che in futuro potresti dover aggiornare o modificare le automazioni basate sull' AWS AppConfig implementazione attuale per motivi di compatibilità.
> Il flag di funzionalità Compute Optimizer -> EC2 instances ha parametri aggiuntivi:
>
> - allow-upscale Per consentire istanze EC2 di fascia alta, sottodimensionate e non ottimizzate. Il valore di default è "false".
> - min-savings-opportunity-percentageL'opportunità percentuale minima di risparmio per la riparazione automatica. Il valore predefinito è 10%

Configurazioni di riparazione predefinite

Le configurazioni per i singoli Trusted Advisor controlli vengono memorizzate come flag. AWS AppConfig Il nome della bandiera corrisponde al nome dell'assegno. Ogni configurazione di controllo contiene i seguenti attributi:

- modalità di esecuzione: determina in che modo Trusted Remediator esegue la correzione predefinita:
  - Automatico: Trusted Remediator corregge automaticamente le risorse creando un documento SSM OpsItem, eseguendo il documento SSM e quindi risolvendo il problema dopo un'esecuzione riuscita. OpsItem

  - Manuale: OpsItem viene creato un documento, ma il documento SSM non viene eseguito automaticamente. Il documento SSM viene esaminato ed eseguito manualmente dalla OpsItem AWS Systems Manager OpsCenter console.
  - Condizionale: la riparazione è disabilitata per impostazione predefinita. È possibile abilitarlo per risorse specifiche utilizzando i tag. Per ulteriori informazioni, vedere le seguenti sezioni Personalizza la riparazione con i tag delle risorse ePersonalizza la riparazione con i tag Resource Override.
  - Inattivo: la riparazione non viene eseguita e non OpsItem viene creata. Non è possibile ignorare la modalità di esecuzione per il Trusted Advisor controllo impostato su inattivo.
- parametri preconfigurati: immettete i valori per i parametri del documento SSM necessari per la riparazione automatica, nel formato di, separati da una virgola (`Parameter=Value`,). Trusted Advisor controlli supportati da Trusted RemediatorPer ogni controllo, vedere i parametri preconfigurati supportati per il documento SSM associato.
- alternative-automation-document: Questo attributo aiuta a sovrascrivere il documento di automazione esistente con un altro documento supportato (se disponibile per il controllo specifico). Per impostazione predefinita, questo attributo non è selezionato.

> **Note**
>
> L'`alternative-automation-document`attributo non supporta documenti di automazione personalizzati. È possibile utilizzare i documenti di automazione Trusted Remediator supportati esistenti elencati inTrusted Advisor controlli supportati da Trusted Remediator.
> Ad esempio, a scopo di controllo`Qch7DwouX1`, ci sono tre documenti SSM associati: AWSManagedServices-StopEC 2Instance, AWSManagedServices-ResizeInstanceByOneLevel e. AWSManagedServices-TerminateInstance Il valore per `alternative-automation-document` può essere AWSManagedServices-ResizeInstanceByOneLevel o AWSManagedServices-TerminateInstance (AWSManagedServices-StopEC2Instance è il documento SSM predefinito da correggere). `Qch7DwouX1`

Il valore di ogni attributo deve corrispondere ai vincoli di tale attributo.

> **Tip**
>
> Prima di applicare le configurazioni predefinite per i Trusted Advisor controlli, è consigliabile prendere in considerazione l'utilizzo delle funzionalità Resource tagging e Resource override descritte nelle sezioni seguenti. Le configurazioni predefinite si applicano a tutte le risorse all'interno dell'account, il che potrebbe non essere consigliabile in tutti i casi.

Di seguito è riportato un esempio di schermata della console con la modalità di esecuzione impostata su Manuale e gli attributi corrispondenti ai relativi vincoli.

Personalizza la riparazione con i tag delle risorse

manual-for-tagged-onlyGli attributi automated-for-tagged-onlyand nella configurazione del controllo consentono di specificare i tag delle risorse relativi al modo in cui si desidera correggere i singoli controlli. È consigliabile utilizzare questo metodo quando è necessario applicare un comportamento di correzione coerente a un gruppo di risorse che condividono lo stesso tag o gli stessi tag. Di seguito sono riportate le descrizioni di questi tag:

- automated-for-tagged-only: Specificate i tag delle risorse (una o più coppie di tag, separate da virgole) per la correzione automatica dei controlli, indipendentemente dalla modalità di esecuzione predefinita.
- manual-for-tagged-only: Specificate i tag delle risorse (una o più coppie di tag, separate da virgole) per le riparazioni che devono essere eseguite manualmente, indipendentemente dalla modalità di esecuzione predefinita.

Ad esempio, se si desidera abilitare la riparazione automatica per tutte le risorse non di produzione e applicare la riparazione manuale per le risorse di produzione, è possibile impostare la configurazione come segue:

```
"execution-mode": "Conditional",
"automated-for-tagged-only": "Environment=Non-Production",
"manual-for-tagged-only": "Environment=Production",
```

Con le configurazioni precedenti impostate sulle risorse, verificate che il comportamento di riparazione sia il seguente:

- Le risorse etichettate con 'Environment=Non-Production' vengono corrette automaticamente.
- Le risorse contrassegnate con 'Environment=Production' richiedono un intervento manuale per la riparazione.
- Le risorse senza il tag 'Environment' seguono la modalità di esecuzione predefinita (`Conditional`, in questo caso. Quindi, non viene intrapresa alcuna azione sulle risorse rimanenti).

Per ulteriore assistenza con le configurazioni, contatta il tuo Cloud Architect.

Personalizza la riparazione con i tag Resource Override

I tag Resource override consentono di personalizzare il comportamento di riparazione per le singole risorse, indipendentemente dai relativi tag. Aggiungendo un tag specifico a una risorsa, si sostituisce la modalità di esecuzione predefinita per quella risorsa e il controllo. Trusted Advisor Il tag resource override ha la precedenza sulla configurazione predefinita e sulle impostazioni di tagging delle risorse. Pertanto, se impostate la modalità di esecuzione predefinita su Automatizzata, Manuale o Condizionale per una risorsa che utilizza il tag Resource Override, questa sovrascrive la modalità di esecuzione predefinita e qualsiasi configurazione di etichettatura delle risorse.

Per sovrascrivere la modalità di esecuzione di una risorsa, completa i seguenti passaggi:

1. Identifica le risorse per le quali desideri sostituire la configurazione di riparazione.
2. Determina l' Trusted Advisor ID del controllo che desideri sostituire. Puoi trovare il controllo IDs per i check-in supportati Trusted Advisor inTrusted Advisor controlli supportati da Trusted Remediator.
3. Aggiungi un tag alle risorse con la chiave e il valore seguenti:
   - Chiave tag: `TR-`*`Trusted Advisor check ID`*`-Execution-Mode` (con distinzione tra maiuscole e minuscole)

     Nell'esempio di chiave del tag precedente, sostituiscilo `Trusted Advisor check ID` con l'identificativo univoco del Trusted Advisor controllo che desideri sovrascrivere.
   - Valore del tag: utilizzate uno dei seguenti valori per il valore del tag:
     - Automatico: Trusted Remediator corregge automaticamente la risorsa per questo Trusted Advisor controllo.
     - Manuale: OpsItem viene creato un file per la risorsa, ma la correzione non viene eseguita automaticamente. La riparazione viene esaminata ed eseguita manualmente da. OpsItem

- Inattivo: la riparazione e OpsItem la creazione non vengono eseguite per questa risorsa e il controllo specificato. Trusted Advisor

Ad esempio, per correggere automaticamente un volume Amazon EBS con l'ID di Trusted Advisor controllo, `DAvU99Dc4C` aggiungi un tag al volume EBS. La chiave del tag è `TR-DAvU99Dc4C-Execution-Mode` e il valore del tag è. `Automated`

Di seguito è riportato un esempio di console che mostra la sezione Tags:

Workflow decisionale in modalità di esecuzione

Esistono diversi livelli per configurare la modalità di esecuzione per le risorse e per ogni Trusted Advisor controllo. Il diagramma seguente mostra come Trusted Remediator decide quale modalità di esecuzione utilizzare in base alle configurazioni:

Configurazione dei tutorial di riparazione

I seguenti tutorial forniscono esempi di creazione di rimedi comuni in Trusted Remediator

Ripristina tutte le risorse manualmente

Questo esempio configura la riparazione manuale per tutti i volumi Amazon EBS con l'ID di Trusted Advisor controllo DAv U99Dc4C (Underutilized Amazon EBS Volumes).

Configura la riparazione manuale per i volumi Amazon EBS con ID di controllo U99Dc4C DAv

1. Apri la console su appconfig. AWS AppConfig https://console.aws.amazon.com/systems-manager/

   Assicurati di accedere come account amministratore delegato.
2. Seleziona Trusted Remediator dall'elenco delle applicazioni.
3. Scegli il profilo di configurazione dell'ottimizzazione dei costi.
4. Seleziona il flag Underutilized Amazon EBS Volumes.
5. Per la modalità di esecuzione, seleziona Manuale.

6. Assicurati che gli manual-for-tagged-onlyattributi automated-for-tagged-onlyand siano vuoti. Questi attributi vengono utilizzati per sovrascrivere la modalità di esecuzione predefinita per le risorse con tag corrispondenti.

   Di seguito è riportato un esempio della sezione Attributi con valori vuoti per automated-for-tagged-onlye manual-for-tagged-onlye Manuale per la modalità di esecuzione:

7. Scegliete Salva per aggiornare il valore, quindi scegliete Salva nuova versione per applicare le modifiche. È necessario scegliere Salva nuova versione affinché Trusted Remediator riconosca la modifica.
8. Assicurati che i tuoi volumi Amazon EBS non abbiano un tag con la chiave`TR-DAvU99Dc4C-Execution-Mode`. Questa chiave di tag sostituisce la modalità di esecuzione predefinita per quel volume EBS.

Ripristina automaticamente tutte le risorse, ad eccezione di quelle selezionate

Questo esempio configura la riparazione automatica per tutti i volumi Amazon EBS con l'ID di Trusted Advisor controllo DAv U99Dc4C (Underutilized Amazon EBS Volumes), ad eccezione dei volumi specificati che non verranno corretti (designati come inattivi).

Configura la riparazione automatica per i volumi Amazon EBS con ID di controllo DAv U99Dc4C, ad eccezione di risorse inattive selezionate

1. AWS AppConfig Apri https://console.aws.amazon.com/systems-manager/la console su appconfig.

   Assicurati di accedere come account amministratore delegato.
2. Seleziona Trusted Remediator dall'elenco delle applicazioni.
3. Scegli il profilo di configurazione dell'ottimizzazione dei costi.
4. Seleziona il flag Underutilized Amazon EBS Volumes.
5. Per la modalità di esecuzione, seleziona Automated.
6. Assicurati che gli manual-for-tagged-onlyattributi automated-for-tagged-onlyand siano vuoti. Questi attributi vengono utilizzati per sovrascrivere la modalità di esecuzione predefinita per le risorse con tag corrispondenti.

   Di seguito è riportato un esempio della sezione Attributi con valori vuoti per automated-for-tagged-onlye manual-for-tagged-onlye Automated for execution-mode:

7. Scegliete Salva per aggiornare il valore, quindi scegliete Salva nuova versione per applicare le modifiche. È necessario scegliere Salva nuova versione affinché Trusted Remediator riconosca la modifica.

   A questo punto, tutti i volumi Amazon EBS sono impostati per la riparazione automatica.
8. Sostituisci la riparazione automatica per volumi Amazon EBS selezionati:

   a. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
   b. Scegli Elastic Block Store, Volumes.
   c. Scegliere Tags (Tag).
   d. Scegliere Gestisci tag.
   e. Aggiungi il seguente tag:

      - Chiave: TR- DAv U99Dc4C-Execution-Mode
      - Valore: inattivo

      Di seguito è riportato un esempio della sezione Tag che mostra i campi Chiave e Valore:

   f. Ripeti i passaggi da 2 a 5 per tutti i volumi Amazon EBS che desideri escludere dalla riparazione.

Correggi automaticamente le risorse contrassegnate

Questo esempio configura la riparazione automatica per tutti i volumi Amazon EBS con il tag `Stage=NonProd` con l'ID di Trusted Advisor controllo DAv U99Dc4C (Underutilized Amazon EBS Volumes). Tutte le altre risorse prive di questo tag non vengono corrette.

Configura la riparazione automatica per i volumi Amazon EBS con il tag **`Stage=NonProd`** per l'ID di controllo U99Dc4C DAv

1. Apri la console su appconfig. AWS AppConfig https://console.aws.amazon.com/systems-manager/

   Assicurati di accedere come account amministratore delegato.
2. Seleziona Trusted Remediator dall'elenco delle applicazioni.

3. Scegli il profilo di configurazione dell'ottimizzazione dei costi.
4. Seleziona il flag Underutilized Amazon EBS Volumes.
5. Per la modalità di esecuzione, seleziona Conditional.
6. Imposta automated-for-tagged-only su `Stage=NonProd`. Questo attributo sostituisce l'impostazione predefinita `execution-mode` per le risorse con tag corrispondenti. Assicurati che manual-for-tagged-onlygli attributi siano vuoti.

   Di seguito è riportato un esempio della sezione Attributi automated-for-tagged-onlyimpostata su Stage= NonProd e Conditional per la modalità di esecuzione:

7. Facoltativamente, impostate i parametri preconfigurati su uno dei seguenti:

   - `CreateSnapshot=false`per non creare snapshot del volume Amazon EBS prima che venga eliminato
   - `MinimumUnattachedDays=10`impostare un numero minimo di giorni non collegati del volume Amazon EBS da eliminare in 10 giorni
   - `CreateSnapshot=false`, `MinimumUnattachedDays=10` per entrambi i casi precedenti
8. Scegli Salva per aggiornare il valore, quindi scegli Salva nuova versione per applicare le modifiche. È necessario scegliere Salva nuova versione affinché Trusted Remediator riconosca la modifica.
9. Assicurati che i tuoi volumi Amazon EBS non abbiano un tag con la chiave`TR-DAvU99Dc4C-Execution-Mode`. Questa chiave di tag sostituisce la modalità di esecuzione predefinita per quel volume EBS.

Lavora con le riparazioni in Trusted Remediator

Tieni traccia delle riparazioni in Trusted Remediator

Per tenere traccia delle OpsItems riparazioni, completa i seguenti passaggi:

1. Apri la AWS Systems Manager console all'indirizzo https://console.aws.amazon.com/systems-manager/.
2. Scegli Operations Management, OpsCenter.
3. (Facoltativo) Filtrate l'elenco per Source=Trusted Remediator per includere solo Trusted OpsItems Remediator nell'elenco.

Di seguito è riportato un esempio della OpsCenter schermata filtrata da Source=Trusted Remediator:

> **Note**
>
> Oltre alla visualizzazione OpsItems da OpsCenter, è possibile visualizzare i registri delle riparazioni nel bucket AMS S3. Per ulteriori informazioni, consulta Registri di riparazione in Trusted Remediator.

Esegui riparazioni manuali in Trusted Remediator

Trusted Remediator crea controlli configurati OpsItems per la riparazione manuale. È necessario rivedere questi controlli e iniziare il processo di riparazione manualmente.

Per rimediare manualmente OpsItem, completa i seguenti passaggi:

1. Apri la AWS Systems Manager console all'indirizzo https://console.aws.amazon.com/systems-manager/.
2. Scegli Operations Management, OpsCenter.
3. (Facoltativo) Filtrate l'elenco per Source=Trusted Remediator per includere solo Trusted OpsItems Remediator nell'elenco.
4. Scegli quello OpsItem che desideri rivedere.
5. Rivedi i dati operativi di OpsItem. I dati operativi includono i seguenti elementi:
   - trustedAdvisorCheckCategoria: la categoria dell'ID dell' Trusted Advisor assegno. Ad esempio, tolleranza ai guasti
   - trustedAdvisorCheckId: l'ID univoco dell' Trusted Advisor assegno.
   - trustedAdvisorCheckMetadati: i metadati della risorsa, incluso l'ID della risorsa.
   - trustedAdvisorCheckNome: il nome dell'assegno. Trusted Advisor
   - trustedAdvisorCheckStato: lo stato del Trusted Advisor controllo rilevato per la risorsa.
6. Per risolvere manualmente il problema OpsItem, completa i seguenti passaggi:
   a. Da Runbook, scegli uno dei runbook associati (documenti SSM).

b. Scegli Esegui.

c. Per AutomationAssumeRole , scegliere `arn:aws:iam::Account AWS ID:role/ams_ssm_automation_role`. Sostituisci Account AWS ID con l'ID dell'account su cui viene eseguita la riparazione. Per altri valori dei parametri, consulta i dati relativi all'operazione.

   Per ripristinare manualmente le risorse, il ruolo o l'utente utilizzato per l'autenticazione Account AWS deve disporre delle `iam:PassRole` autorizzazioni per il ruolo IAM. `ams-ssm-automation-role` Per ulteriori informazioni, consulta Concedere a un utente le autorizzazioni per trasferire un ruolo a un utente Servizio AWS o contatta il tuo Cloud Architect.

d. Scegli Esegui.

e. Monitora l'avanzamento dell'esecuzione del documento SSM nella colonna Stato e risultati più recenti.

f. Una volta completato il documento, scegli Imposta stato, Risolto per risolvere manualmente il. OpsItem Se il documento ha avuto esito negativo, rivedi i dettagli ed esegui nuovamente il. SSMdocument Per ulteriore assistenza nella risoluzione dei problemi, crea una richiesta di assistenza.

Per risolvere un problema OpsItem senza riparazione, seleziona Imposta lo stato su Risolto.

7. Ripeti i passaggi 3 e 4 per tutte le riparazioni OpsItems manuali rimanenti.

Risolvi i problemi relativi alle riparazioni in Trusted Remediator

Per assistenza sulle riparazioni manuali e sugli errori di riparazione, contatta AMS.

Per visualizzare lo stato e i risultati della riparazione, completa i seguenti passaggi:

1. Apri la AWS Systems Manager console all'indirizzo https://console.aws.amazon.com/systems-manager/.
2. Scegli Operations Management, OpsCenter.
3. (Facoltativo) Filtrate l'elenco per Source=Trusted Remediator per includere solo Trusted OpsItems Remediator nell'elenco.
4. Scegli quello OpsItem che desideri rivedere.
5. Nella sezione Automation Executions, esamina il nome, lo stato del documento e i risultati.

6. Esamina i seguenti errori di automazione comuni. Se i tuoi problemi non sono elencati qui, contatta il tuo CSDM per ricevere assistenza.

Errori di riparazione comuni

Nessuna esecuzione è elencata in Automation Executions

Nessuna esecuzione associata a OpsItem potrebbe indicare che l'esecuzione non è stata avviata a causa di valori dei parametri errati.

Fasi per la risoluzione dei problemi

1. Nei Dati operativi, esamina il valore della `trustedAdvisorCheckAutoRemediation` proprietà.
2. Verificate che i valori DocumentNamee Parameters siano corretti. Per i valori corretti, Configurare Trusted Advisor la correzione degli assegni in Trusted Remediator consulta i dettagli su come configurare i parametri SSM. Per esaminare i parametri di controllo supportati, vedere Trusted Advisor controlli supportati da Trusted Remediator
3. Verifica che i valori nel documento SSM corrispondano ai modelli consentiti. Per visualizzare i dettagli dei parametri nel contenuto del documento, seleziona il nome del documento nella sezione Runbooks.
4. Dopo aver esaminato e corretto i parametri, esegui nuovamente manualmente il documento SSM.
5. Per evitare che questo errore si ripresenti, assicuratevi di configurare la riparazione con i valori dei parametri corretti nella configurazione. Per ulteriori informazioni, consulta Configurare Trusted Advisor la correzione degli assegni in Trusted Remediator

Esecuzioni non riuscite in Automation Executions

I documenti di riparazione contengono più passaggi che interagiscono con l' Servizi AWS esecuzione di varie azioni. APIs Per identificare una causa specifica dell'errore, completa i seguenti passaggi:

Fasi per la risoluzione dei problemi

1. Per visualizzare i singoli passaggi di esecuzione, scegli l'ID di esecuzione, link nella sezione Automation Executions. Di seguito è riportato un esempio della console Systems Manager che mostra i passaggi di esecuzione per un'automazione selezionata:

2. Scegli il passaggio con lo stato Non riuscito. Di seguito sono riportati alcuni esempi di messaggi di errore:

   - `NoSuchBucket - An error occurred (NoSuchBucket) when calling the GetPublicAccessBlock operation: The specified bucket does not exist`

     Questo errore indica che il nome errato del bucket è stato specificato nei parametri preconfigurati della configurazione di riparazione.

     Per risolvere questo errore, esegui manualmente l'automazione utilizzando il nome del bucket corretto. Per evitare che questo problema si ripresenti, aggiorna la configurazione di riparazione con il nome del bucket corretto.
   - `DB instance my-db-instance-1 is not in available status for modification.`

     Questo errore indica che l'automazione non è riuscita ad apportare le modifiche previste perché l'istanza DB si trovava in uno stato non valido.

     Per risolvere questo errore, esegui manualmente l'automazione.

Registri di riparazione in Trusted Remediator

Trusted Remediator crea log in formato JSON e li carica su Amazon Simple Storage Service. I file di log vengono caricati in un bucket S3 creato da AMS e denominato. `ams-trusted-remediator-{your-account-id}-logs` AMS crea il bucket S3 nell'account Delegated Administrator. È possibile importare i file di registro in Quick per generare report di riparazione personalizzati.

Per ulteriori informazioni, consulta Integrazione di Trusted Remediator con Quick.

Registro degli elementi di riparazione

Trusted Remediator crea il `Remediation item log` momento in cui viene creata una riparazione OpsItem . Questo registro contiene la riparazione manuale OpsItem e la riparazione automatica. OpsItem È possibile utilizzare il file `Remediation item log` per tenere traccia della panoramica di tutte le riparazioni.

Posizione del registro degli elementi di riparazione per i consigli di Compute Optimizer

`s3://ams-trusted-remediator-`*`delegated-administrator-account-id`*`-logs/compute_optimizer_remediation_items/`*`remediation creation time in yyyy-mm-dd`*

format/*10 digits epoch time or unix timestamp*-*Compute Optimizer check ID*-*Resource ID*.json

Posizione del registro degli elementi di riparazione per i controlli Trusted Advisor

s3://ams-trusted-remediator-*delegated-administrator-account-id*-logs/remediation_items/*remediation creation time in yyyy-mm-dd format*/*10 digits epoch time or unix timestamp*-*Trusted Advisor check ID*- *Resource ID*.json

Posizione del registro degli elementi di riparazione per i consigli CSPM di Security Hub

s3://ams-trusted-remediator-*delegated-administrator-account*-id-logs/security_hub_remediation_items/*remediation creation time in yyyy-mm-dd format*/*10 digits epoch time or unix timestamp-Security Hub CSPM check ID-Resource ID*.json

URL di esempio del file di registro dell'elemento di riparazione

s3:///ams-trusted-remediator-*111122223333*-logs/remediation_items/*2023-02-06*/*1675660464-DAvU99Dc4C-vol-00bd8965660b4c16d.json*

Formato di registro degli elementi di Compute Optimizer Remediation

```
{
  "AccountID": "Account_ID",
  "ComputeOptimizerCheckID": "Compute Optimizer check ID",
  "ComputeOptimizerCheckName": "Compute Optimizer check name",
  "ResourceID": "Resource ID",
  "RemediationTime": Remediation creation time,
  "ExecutionMode": "Automated or Manual",
  "OpsItemID": "OpsItem ID"
}
```

Trusted Advisor Formato del registro degli elementi di riparazione

```
{
   "TrustedAdvisorCheckID": Trusted Advisor check ID,
   "TrustedAdvisorCheckName": Trusted Advisor check name,
   "TrustedAdvisorCheckResultTime": 10 digits epoch time or unix timestamp,
   "ResourceID": Resource ID,
```

```
   "RemediationTime": Remediation creation time,
   "ExecutionMode": Automated or Manual,
   "OpsItemID": OpsItem ID
}
```

Formato di registro degli elementi di riparazione CSPM di Security Hub

```
{
 "AccountID": "Account_ID",
 "SecurityHubCheckID": "Security Hub check ID",
 "SecurityHubCheckName": "Security Hub check name",
 "ResourceID": "Resource ID",
 "RemediationTime": Remediation creation time,
 "ExecutionMode": "Automated or Manual",
 "OpsItemID": "OpsItem ID"
}
```

Contenuto di esempio in formato di log dell'elemento Compute Optimizer Remediation

```
{
  "AccountID": "123456789012",
  "ComputeOptimizerCheckID": "compute-optimizer-ebs",
  "ComputeOptimizerCheckName": "EBS volumes",
  "ResourceID": "vol-1235589366f77aca7",
  "RemediationTime": 1755044783,
  "ExecutionMode": "Manual",
  "OpsItemID": "oi-b8888b38fe78"
}
```

Trusted Advisor Contenuto di esempio del formato del registro degli elementi di riparazione

```
{
    "TrustedAdvisorCheckID": "DAvU99Dc4C",
    "TrustedAdvisorCheckName": "Underutilized Amazon EBS Volumes",
    "TrustedAdvisorCheckResultTime": 1675614749,
    "ResourceID": "vol-00bd8965660b4c16d",
    "RemediationTime": 1675660464,
    "OpsItemID": "oi-cca5df7af718"
}
```

Contenuto di esempio del formato di registro degli elementi di riparazione CSPM di Security Hub

```
{
    "AccountID": "012345678901",
    "SecurityHubControlID": "security-hub-lambda-7",
    "SecurityHubControlName": "Lambda functions should have AWS X-Ray active tracing
 enabled",
    "SecurityHubControlResultTime": 1764580147,
    "ResourceID": "test-lambda-7-xray-disabled",
    "RemediationTime": 1764900171,
    "ExecutionMode": "Manual",
    "OpsItemID": "oi-ea12c3456d7f"
}
```


Registro di esecuzione della riparazione automatizzata, Compute Optimizer, Security Hub CSPM e Trusted Advisor

Trusted Remediator crea il `Automated remediation execution log` quando viene completata l'esecuzione automatica di un documento SSM. Questo registro contiene i dettagli dell'esecuzione di SSM solo per la riparazione automatica. OpsItem È possibile utilizzare questo file di registro per tenere traccia delle riparazioni automatiche.

Compute Optimizer Posizione del registro di correzione automatizzata

`s3://ams-trusted-remediator-`*`delegated-administrator-account-id`*`-logs//remediation_executions/`*`remediation creation time in yyyy-mm-dd format`*`/`*`10 digits epoch time or unix timestamp`*`-`*`Compute Optimizer recommendation ID`*`.json`

Security Hub CSPM Posizione del registro di riparazione automatizzato

`s3://ams-trusted-remediator-`*`delegated-administrator-account-id`*`-logs//remediation_executions/`*`remediation creation time in yyyy-mm-dd format`*`/`*`10 digits epoch time or unix timestamp`*`-`*`Security Hub CSPM recommendation ID`*`.json`

Trusted Advisor Posizione del registro di riparazione automatizzato

`s3://ams-trusted-remediator-`*`delegated-administrator-account-id`*`-logs//remediation_executions/`*`remediation creation time in yyyy-mm-dd format`*`/`*`10 digits epoch time or unix timestamp`*`-`*`Trusted Advisor check ID`*`-`*`Resource ID`*`.json`

Esempio di posizione del registro di correzione automatizzato di Compute Optimizer

`s3://ams-trusted-remediator-111122223333-logs/remediation_executions/2025-06-26/1750908858-123456789012-compute-optimizer-ec2-i-1235173471d2cd789.json`

Security Hub CSPM Esempio di posizione del registro di riparazione automatizzato

`s3://ams-trusted-remediator-111122223333-logs/remediation_executions/2025-06-26/763247655-066028476520-security-hub-rds-8-miz-tr-sh-test-rds-instance-1.json`

Trusted Advisor Esempio di posizione del registro di riparazione automatizzato

`s3://ams-trusted-remediator-111122223333-logs/remediation_executions/2023-02-06/1675660573-DAvU99Dc4C-vol-00bd8965660b4c16d.json`

Contenuto di esempio in formato registro di riparazione automatizzato

```
{
    "OpsItemID": "oi-767c77e05301",
    "SSMExecutionID": "93d091b2-778a-4cbc-b672-006954d76b86",
    "SSMExecutionStatus": "Success"
}
```

Registro degli account dei membri

Trusted Remediator crea il messaggio `Member accounts log` quando il tuo account viene inserito o abbandonato. Puoi utilizzare il `Member accounts log` per trovare l'ID dell'account, l'iscrizione e l'ora di esecuzione di ciascun account Regioni AWS membro.

Posizione dei registri degli account dei membri

`s3://ams-trusted-remediator-delegated-administrator-account-id-logs/configuration_logs/member_accounts.json`

URL di esempio del file di registro degli account membri

`s3://ams-trusted-remediator-111122223333-logs/configuration_logs/member_accounts.json`

Formato di registro degli account dei membri

```
{
    "delegated_administrator_account_id": Delegated Administrator account id,
    "appconfig_configuration_region": Trusted Remediator AppConfig Region,
    "member_accounts": [
        {
            "account_id": Member account id
            "account_partition": Member account partition (for example, aws),
            "regions": [
                {
                    "execution_time": Remediation execution time in cron schedule
 expression,
                    "execution_timezone": Timezone for the remediation execution time,
                    "region_name": Regione AWS name
                }
                ...
            ]
        }
        ...
    ],
    "updated_at": Log update time,
}
```

Contenuto di esempio del formato di registro degli account dei membri

```
{
    "delegated_administrator_account_id": "111122223333",
    "appconfig_configuration_region": "ap-southeast-2",
    "member_accounts": [
        {
            "account_id": "222233334444",
            "account_partition": "aws",
            "regions": [
                {
                    "execution_time": "0 9 * * 6",
                    "execution_timezone": "Australia/Sydney",
                    "region_name": "ap-southeast-2"
                },
                {
                    "execution_time": "0 5 * * 7",
                    "execution_timezone": "UTC",
                    "region_name": "us-east-1"
```

```
                }
            ]
        },
        {
            "account_id": "333344445555",
            "account_partition": "aws",
            "regions": [
                {
                    "execution_time": "0 1 * * 5",
                    "execution_timezone": "Asia/Seoul",
                    "region_name": "ap-northeast-2"
                }
            ]
        }
    ],
    "updated_at": "1730869607"
}
```

Integrazione di Trusted Remediator con Quick

Puoi integrare i log di Trusted Remediator archiviati in Amazon S3 con Quick per creare report di riparazione personalizzati. L'integrazione rapida è facoltativa. Questa funzionalità consente di utilizzare i log per creare dashboard di reporting personalizzati. Per ottenere report su richiesta per Trusted Remediator, contattate il vostro CSDM. Per ulteriori informazioni sui report Trusted Remediator disponibili, consulta. Report di Trusted Remediator

Per ulteriori informazioni sulla visualizzazione dei dati in Quick, consulta Visualizzazione dei dati in Quick.

Aggiungi un set di dati al registro degli elementi di Quick for the Remediation

Per aggiungere un set di dati al registro degli elementi di Quick for the Remediation, segui questi passaggi:

1. Accedere alla console Quick. È possibile creare il rapporto rapido in qualsiasi formato supportato da Regione AWS Quick. Tuttavia, per migliorare le prestazioni e ridurre i costi, è consigliabile creare il report nella regione in cui si trova il bucket di registrazione Trusted Remediator.
2. Scegli Set di dati.
3. Scegli S3.
4. Nella nuova origine dati S3, inserisci i seguenti valori:

- Nome della fonte di dati: `trusted-remediator-`*`delegated_administrator_account_id`*`-`*`account_region`*`-remediation-items`.
- Carica un file manifest: crea un file JSON con il seguente contenuto e usalo. Quando crei il file, `logging_bucket_name` sostituiscilo nella URIPrefixes chiave.

```
{
    "fileLocations": [
        {
            "URIPrefixes": [
                "s3://{logging_bucket_name}/remediation_items/"
            ]
        }
    ],
    "globalUploadSettings": {
        "format": "JSON",
        "delimiter": ",",
        "textqualifier": "'",
        "containsHeader": "true"
    }
}
```

- Scegli Connetti.
- Nella finestra Termina la creazione del set di dati, scegli Visualizza.
- Quick apre la nuova pagina del foglio di analisi. Ora sei pronto per creare una nuova analisi utilizzando il registro degli elementi di riparazione.

Di seguito è riportato un esempio di analisi:

Aggiungere un set di dati al registro di esecuzione della riparazione automatica di Quick for the Automated Remediation

1. Accedi alla console Quick. È possibile creare il rapporto rapido in qualsiasi formato supportato da Regione AWS Quick. Tuttavia, per migliorare le prestazioni e ridurre i costi, è consigliabile creare il report nella regione in cui si trova il bucket di registrazione Trusted Remediator.
2. Scegli Set di dati.
3. Scegli S3.

4. Nella nuova origine dati S3, inserisci i seguenti valori:

   - Nome della fonte di dati:`trusted-remediator-`*`delegated_administrator_account_id`*`-`*`account_region`*`-remediation-executions`.
   - Carica un file manifest: crea un file JSON con il seguente contenuto, quindi utilizza questo file. Quando crei il file, `logging_bucket_name` sostituiscilo nella URIPrefixes chiave.

     ```
     {
         "fileLocations": [
             {
                 "URIPrefixes": [
                     "s3://{logging_bucket_name}/remediation_executions/"
                 ]
             }
         ],
         "globalUploadSettings": {
             "format": "JSON",
             "delimiter": ",",
             "textqualifier": "'",
             "containsHeader": "true"
         }
     }
     ```

   - Scegli Connetti.
   - Nella finestra Termina la creazione del set di dati, scegli Visualizza.
   - Quick apre la nuova pagina del foglio di analisi. Ora sei pronto per creare una nuova analisi utilizzando il registro degli elementi di riparazione.

Di seguito è riportato un esempio di analisi:

Le migliori pratiche in Trusted Remediator

Di seguito sono riportate le best practice per aiutarti a utilizzare Trusted Remediator:

- Se non sei sicuro dei risultati della correzione, inizia con la modalità di esecuzione manuale. A volte, applicare l'esecuzione automatizzata per le riparazioni sin dall'inizio potrebbe causare risultati imprevisti.

- Esegui una revisione settimanale delle correzioni e approfondisci OpsItems i risultati di Trusted Remediator.
- Gli account membro ereditano le configurazioni dall'account amministratore delegato. Pertanto, è importante strutturare gli account in modo da gestire più account con le stesse configurazioni. È possibile esentare le risorse dalla configurazione predefinita utilizzando i tag.

Trusted Remediator FAQs

Di seguito sono riportate le domande frequenti su Trusted Remediator:

Che cos'è Trusted Remediator e quali sono i miei vantaggi?

Quando viene identificata una non conformità Trusted Advisor o viene emessa una raccomandazione da Compute Optimizer o Security Hub CSPM, Trusted Remediator risponde in base alle preferenze specificate, applicando la correzione, richiedendo l'approvazione tramite riparazioni manuali o segnalando le correzioni durante la prossima Monthly Business Review (MBR). La riparazione viene eseguita all'orario o al programma di riparazione preferiti. Trusted Remediator offre la possibilità di eseguire operazioni self-service e intervenire in base ai Trusted Advisor controlli con la flessibilità necessaria per configurare e correggere i controlli singolarmente o in blocco. Con una libreria di documenti di correzione testati, AMS aumenta costantemente la tua reputazione applicando controlli di sicurezza e seguendo le migliori pratiche. AWS Riceverete una notifica solo se specificate di farlo nella configurazione. Gli utenti AMS possono optare per Trusted Remediator senza costi aggiuntivi.

In che modo Trusted Remediator si relaziona e funziona con gli altri? Servizi AWS

Hai accesso ai Trusted Advisor controlli, ai consigli di Compute Optimizer e ai controlli CSPM di Security Hub come parte del tuo piano Enterprise Support esistente. Trusted Remediator si integra con Trusted Advisor Compute Optimizer e Security Hub CSPM per sfruttare le funzionalità di automazione AMS esistenti. In particolare, AMS utilizza documenti di AWS Systems Manager automazione (runbook) per le riparazioni automatiche. AWS AppConfig viene utilizzato per configurare i flussi di lavoro di riparazione. È possibile visualizzare tutte le riparazioni attuali e passate tramite Systems Manager OpsCenter. I log di riparazione sono archiviati in un bucket Amazon S3. Puoi utilizzare i log per importare e creare dashboard di reporting personalizzate in Quick.

Chi configura le riparazioni?

Sei il proprietario delle configurazioni del tuo account. La gestione delle configurazioni è responsabilità dell'utente. Puoi contattare il tuo CA o il CDSM per ricevere assistenza nella gestione

delle configurazioni. Puoi anche contattare AMS tramite una richiesta di servizio per il supporto alla configurazione, le riparazioni manuali e la risoluzione degli errori di riparazione.

Come posso installare i documenti di automazione SSM?

I documenti di automazione SSM vengono condivisi automaticamente con gli account AMS registrati.

Verranno ripristinate anche le risorse di proprietà di AMS?

Le risorse di proprietà di AMS non sono contrassegnate da Trusted Remediator. Trusted Remediator si concentra solo sulle tue risorse.

In cosa Regioni AWS è disponibile Trusted Remediator e chi può utilizzarlo?

Trusted Remediator è disponibile per i clienti AMS Accelerate. Per un elenco aggiornato delle regioni di supporto, vedi Servizi AWS per regione.

Trusted Remediator causerà la deriva delle risorse?

Poiché i documenti di automazione SSM aggiornano direttamente le risorse tramite l' AWS API, potrebbe verificarsi una deriva delle risorse. È possibile utilizzare i tag per separare le risorse create tramite i pacchetti esistenti. CI/CD È possibile configurare Trusted Remediator in modo che ignori le risorse contrassegnate continuando a correggere le altre risorse.

Come posso mettere in pausa o interrompere Trusted Remediator?

È possibile disattivare Trusted Remediator tramite l'applicazione. AWS AppConfig Per mettere in pausa o interrompere Trusted Remediator, completa i seguenti passaggi:

1. Apri la AWS AppConfig console all'indirizzo https://console.aws.amazon.com/systems-manager/appconfig.
2. Seleziona Trusted Remediator.
3. Scegli Impostazioni nel profilo di configurazione.
4. Seleziona il flag Suspend Trusted Remediator.
5. Imposta il valore dell'attributo su. `suspended` `true`

> **Note**
>
> Prestare attenzione quando si utilizza questa procedura poiché interrompe Trusted Remediator per tutti gli account collegati all'account amministratore delegato.

Come posso correggere i controlli che non sono supportati da Trusted Remediator?

Puoi continuare a contattare AMS tramite Operations On Demand (OOD) per i controlli non supportati. AMS ti aiuta a correggere questi controlli. Per ulteriori informazioni, consulta Operations On Demand.

In che modo Trusted Remediator è diverso dalla AWS Config riparazione?

AWS Config Remediation è un'altra soluzione che ti aiuta a ottimizzare le risorse cloud e a mantenere la conformità con le migliori pratiche. Di seguito sono riportate alcune delle differenze operative tra le due soluzioni:

- Trusted Remediator utilizza Trusted Advisor Compute Optimizer e Security Hub CSPM come meccanismi di rilevamento. AWS Config Remediation utilizza AWS Config le regole come meccanismo di rilevamento.
- Per Trusted Remediator, la riparazione avviene secondo la pianificazione di riparazione predefinita. Nel AWS Config, la riparazione avviene in tempo reale.
- I parametri per ogni riparazione in Trusted Remediator sono facilmente personalizzabili in base al caso d'uso e la riparazione può essere automatizzata o resa manuale aggiungendo tag alle risorse.
- Trusted Remediator offre funzionalità di reporting.
- Trusted Remediator invia all'utente una notifica via e-mail con l'elenco delle misure correttive e lo stato della riparazione.

Alcuni Trusted Advisor controlli, i consigli di Compute Optimizer e Security Hub CSPM potrebbero includere la stessa regola. AWS ConfigÈ consigliabile abilitare una sola correzione se esistono una regola e un controllo corrispondenti. AWS Config Trusted Advisor Per informazioni sulle AWS Config regole per ogni Trusted Advisor controllo, consultaTrusted Advisor controlli supportati da Trusted Remediator.

Quali risorse distribuisce Trusted Remediator ai tuoi account?

Trusted Remediator distribuisce le seguenti risorse nell'account amministratore delegato di Trusted Remediator:

- Un bucket Amazon S3 denominato. `ams-trusted-remediator-{your-account-id}-logs` Trusted Remediator crea il file `Remediation item log` in formato JSON quando OpsItem viene creata una correzione e carica i file di registro in questo bucket.

- Un' AWS AppConfig applicazione per contenere le configurazioni di riparazione per i Trusted Advisor controlli supportati, i consigli CSPM di Compute Optimizer e Security Hub.

Trusted Remediator non distribuisce risorse nell'account membro di Trusted Remediator.

Monitoraggio e gestione degli incidenti per Amazon EKS in AMS Accelerate

Il monitoraggio e la gestione degli incidenti per Amazon EKS monitora le risorse Amazon EKS per individuare guasti, peggioramento delle prestazioni e problemi di sicurezza. AMS Accelerate configura e implementa le regole di gestione degli avvisi di Amazon Managed Service for Prometheus, monitora gli avvisi e quindi esegue la gestione degli incidenti quando questi avvisi vengono attivati. Il monitoraggio e la gestione degli incidenti per Amazon EKS si basano su AMS Alarm Manager e sfrutta AWS servizi nativi, come Amazon Managed Service for Prometheus, Amazon Managed Grafana, Amazon e. GuardDuty AWS LambdaAWS Config

> **Important**
>
> Il monitoraggio e la gestione degli incidenti per Amazon EKS non supportano la regione Asia Pacifico (Malesia) AWS GovCloud (US), i nodi Windows o i contenitori Windows.

Che cos'è il monitoraggio e la gestione degli incidenti per Amazon EKS in AMS Accelerate?

Il monitoraggio e la gestione degli incidenti per Amazon EKS forniscono quanto segue:

- Una configurazione predefinita che crea, gestisce e distribuisce monitor e policy nel tuo account gestito per i cluster Amazon EKS da te selezionati.
- Una base di monitoraggio per consentire ai carichi di lavoro Amazon EKS di avere una maggiore disponibilità, anche se non configuri nessun altro monitoraggio per i tuoi cluster Amazon EKS. Per ulteriori informazioni, consulta Avvisi di base per il monitoraggio e la gestione degli incidenti per Amazon EKS in AMS Accelerate.
- Notifiche generate dal monitoraggio di base configurato per il tuo cluster Amazon EKS. Queste notifiche sono note come avvisi. Gli avvisi vengono generati in caso di guasti imminenti, continui, ricorrenti o potenziali, peggioramento delle prestazioni o problemi di sicurezza. Esempi di avvisi includono un avviso Prometheus, un evento o una scoperta da un servizio, come Amazon. AWS GuardDuty

- Indagine sugli avvisi con indicazioni sulle azioni correttive appropriate che è possibile intraprendere. Per ulteriori informazioni, consulta Segnalazioni di incidenti e richieste di assistenza in AMS Accelerate.
- Correzione di avvisi e incidenti da parte delle operazioni AMS, quando possibile e con la tua approvazione, per prevenire o ridurre l'impatto sulle tue applicazioni. Per ulteriori informazioni, consulta Segnalazioni di incidenti e richieste di assistenza in AMS Accelerate.
- Dashboard Amazon Managed Grafana predefinite opzionali che forniscono visibilità sull'utilizzo delle risorse, sulle prestazioni, sullo stato di CoredNS, sugli avvisi attivi e sugli avvisi precedentemente risolti. Se configuri Amazon Managed Grafana utilizzando il modello fornito da AMS, puoi aprire la console Amazon Managed Grafana per visualizzare metriche e avvisi per il tuo cluster Amazon EKS.

Come funzionano il monitoraggio e la gestione degli incidenti per Amazon EKS in AMS Accelerate

Generazione: nell'ambito del monitoraggio dell'onboarding e della gestione degli incidenti per EKS, AMS configura il monitoraggio di base per i cluster Amazon EKS selezionati nel tuo account gestito. AMS utilizza una combinazione delle regole di gestione degli avvisi di Amazon Managed Service for Prometheus e delle regole degli eventi di CloudWatch Amazon per configurare il monitoraggio di base. Un server Prometheus configurato con AMS nel tuo cluster esegue lo scraping e scrive in remoto i parametri Prometheus su un endpoint Amazon Managed Service for Prometheus nella stessa regione. La configurazione di monitoraggio di base genera un avviso quando viene attivata una regola di Prometheus alert manager o viene generato un evento. CloudWatch

Aggregazione: AMS invia tutti gli avvisi generati dalle tue risorse al sistema di monitoraggio AMS indirizzandoli a un argomento di Amazon Simple Notification Service gestito da AMS.

Elaborazione e analisi dell'impatto: AMS analizza gli avvisi e li elabora in base al loro potenziale impatto. AMS classifica gli avvisi come segue:

- Avvisi con impatto noto sui clienti: per questi avvisi, AMS crea un nuovo rapporto sugli incidenti utilizzando il processo di gestione degli incidenti.
- Avvisi con impatto incerto sui clienti: per questi avvisi, AMS invia un rapporto sugli incidenti. In molti casi, questi avvisi richiedono di verificare l'impatto prima che AMS possa intervenire. Per tali avvisi, AMS invia una notifica di avviso con i dettagli e verifica se l'avviso necessita di un'azione attenuante. AMS offre opzioni per mitigare le azioni nella notifica. Se la risposta conferma che

l'avviso è un incidente, AMS avvia la creazione di un nuovo rapporto sull'incidente e avvia il processo di gestione dell'incidente. Qualsiasi notifica di servizio che riceve una risposta di «nessun impatto sul cliente» o nessuna risposta per tre giorni viene contrassegnata come risolta. Inoltre, l'avviso corrispondente viene contrassegnato come risolto.

- Avvisi senza impatto sul cliente: se, dopo la valutazione, AMS determina che l'avviso non ha alcun impatto sul cliente, l'avviso viene chiuso.

Matrice di responsabilità AMS (RACI)

La matrice AMS responsabile, responsabile, consultata e informata, o RACI, assegna la responsabilità principale al cliente o ad AMS per una serie di attività. La tabella seguente fornisce una panoramica delle responsabilità del cliente e di AMS per le attività in un'applicazione che utilizza Monitoring and Incident Management per Amazon EKS.

- R sta per la parte responsabile che svolge il lavoro per raggiungere l'obiettivo.
- A sta per parte responsabile.
- C sta per consultata; la parte i cui pareri vengono richiesti, generalmente in qualità di esperti in materia, e con la quale esiste una comunicazione bilaterale.
- I sta per informato; la parte che viene informata sui progressi, spesso solo al completamento del compito o del risultato.

Attività	Customer	AMS
Requisiti Discovery for AMS	I	R
Abilita le autorizzazioni AMS (RBAC) per l'accesso al cluster	R	C
Installa Amazon EC2 Systems Manager Agent sui nodi di lavoro se non è già presente	R	C
Implementa componenti AMS su cluster, come Prometheu s, Prometheus Node Exporter	C	R

Attività	Customer	AMS
e in un namespace AMS, in base alle esigenze. kube-state-metrics		
Fornisci Amazon Managed Service per Prometheus nel piano di controllo AMS	I	R
Configurare Prometheus alert manager nel piano di controllo AMS	I	R
Fornisci il modello Amazon Managed Grafana e assisti nella configurazione	C	R
Abilita il monitoraggio dei log di audit GuardDuty EKS	C	R
Abilita la registrazione del piano di controllo Amazon EKS	I	R
Monitora lo stato e le prestazioni del piano di controllo di Amazon EKS	I	R
Monitora lo stato e le prestazioni del tuo cluster Amazon EKS (cluster, nodo, carico di lavoro, pod, API Server e CoredNS)	I	R
Valuta gli avvisi e fornisci una risposta agli incidenti per Amazon EKS	I	R

Attività	Customer	AMS
Esegui comandi diagnostici durante gli incidenti	I	R
Analizza i log durante gli incidenti (log del piano di controllo e dei pod)	I	R
Risposta agli incidenti per problemi di rete AWS	I	R
Rispondi ai risultati di GuardDuty EKS Audit Log Monitoring	I	R
Fornisci ai clienti indicazioni sulle azioni da intraprendere per porre rimedio agli incidenti quando possibile	I	R

Avvisi di base per il monitoraggio e la gestione degli incidenti per Amazon EKS in AMS Accelerate

Dopo aver verificato gli avvisi, AMS abilita i seguenti avvisi per Amazon EKS e quindi si occupa del monitoraggio e della gestione degli incidenti per i cluster Amazon EKS selezionati. I tempi di risposta Service Level Agreements (SLAs) e Service Level Objectives (SLOs) dipendono dal livello di servizio (Plus, Premium) dell'account selezionato. Per ulteriori informazioni, consulta Segnalazioni di incidenti e richieste di assistenza in AMS Accelerate.

Avvisi e azioni

La tabella seguente elenca gli avvisi di Amazon EKS e le rispettive azioni intraprese da AMS:

Alert	Soglie	Azione
Container OOM ucciso	Il numero totale di riavvii dei container negli ultimi 10 minuti è almeno 1 e un container Kubernetes in un pod è stato chiuso con il motivo «OOMKilled» negli ultimi 10 minuti.	AMS verifica se il blocco dell'OOM è causato dal raggiungimento del limite del contenitore o dall'overcommit del limite di memoria, quindi consiglia all'utente le azioni correttive necessarie.
Pod Job non riuscito	Un job Kubernetes non viene completato. L'errore è indicato dalla presenza di almeno uno stato di lavoro non riuscito.	AMS analizza il motivo per cui il job Kubernetes o il cron job corrispondente non funziona correttamente, quindi consiglia all'utente le azioni correttive.
StatefulSet Giù	Il numero di repliche pronte a servire il traffico non corrispon de al numero attuale di repliche esistenti StatefulSet per almeno 1 minuto.	AMS determina il motivo per cui i pod non sono pronti esaminando i messaggi di errore negli eventi dei pod e i frammenti di registro degli errori nei log dei pod, quindi consiglia all'utente le azioni correttive.
Capacità di scalabilità HPA	L'Horizontal Pod Autoscale r (HPA) non è in grado di scalare perché la condizione di stato «AbleToScale» è falsa per almeno 2 minuti.	AMS determina quale Kubernetes Horizontal Pod Autoscaler (HPA) non è in grado di scalare i pod per la successiva risorsa del carico di lavoro, ad esempio un Deployment o. StatefulSet
Disponibilità metrica HPA	Horizontal Pod Autoscale r (HPA) non è in grado di raccogliere metriche perché la condizione di stato «ScalingA	AMS determina il motivo per cui HPA non è in grado di raccogliere metriche, ad esempio metriche relative a

Alert	Soglie	Azione
	ctive» è falsa da almeno 2 minuti.	problemi di configurazione del server o problemi di autorizza zione RBAC.
Pod non pronto	Un pod Kubernetes rimane in uno stato non in esecuzion e (ad esempio Pending, Unknown o Failed) per più di 15 minuti.	AMS esamina i pod interessati per ulteriori dettagli, esamina i log dei pod alla ricerca di errori ed eventi correlati e quindi consiglia all'utente le azioni correttive necessarie.
Pod Crash Looping	Un contenitore di pod si riavvia almeno una volta ogni 15 minuti per un periodo di 1 ora.	AMS analizza i motivi del mancato avvio del pod, ad esempio risorse insuffici enti, un file bloccato da un altro contenitore, il database bloccato da un altro contenito re, errori nelle dipendenze del servizio, problemi DNS per i servizi esterni e configurazioni errate.
Daemonset è programmato in modo errato	C'è almeno un pod Kubernete s Daemonset programmato in modo errato nell'arco di 10 minuti.	AMS determina il motivo per cui un Daemonset è pianifica to su un nodo in cui non dovrebbe essere eseguito. Ciò potrebbe accadere quando il pod sbagliato nodeSelec tor/taints/affinities veniva applicato ai pod Daemonset o quando il nodo (pool di nodi) era contaminato e i pod esistenti non erano programmati per lo sfratto.

Alert	Soglie	Azione
Errori dell'API Kubernetes	Il tasso di errore del server dell'API Kubernetes supera il 3% in un periodo di 2 minuti.	AMS analizza i log del piano di controllo per determina re il volume e i tipi di errori che causano questo avviso e identifica eventuali problemi di contesa delle risorse per i gruppi di scalabilità automatic a del nodo master o di etcd. Se il server API non si ripristin a, AMS contatta il team di assistenza Amazon EKS.
Latenza dell'API Kubernetes	La latenza del 99° percentile delle richieste al server API Kubernetes supera 1 secondo in un periodo di 2 minuti.	AMS analizza i log del piano di controllo per determinare il volume e i tipi di errori che causano la latenza e identifica eventuali problemi di conflitto di risorse per i nodi master o i gruppi di auto-scaling etcd. Se il server API non si ripristin a, AMS contatta il team di assistenza Amazon EKS.
Certificato client Kubernetes in scadenza	Il certificato client utilizzato per l'autenticazione sul server API Kubernetes scadrà tra meno di 24 ore.	AMS invia questa notifica per informarti che il certificato del cluster scadrà tra 24 ore.
Nodo non pronto	Lo stato della condizione «Pronto» del nodo è falso per almeno 10 minuti.	AMS analizza le condizion i e gli eventi del nodo, come i problemi di rete, che impediscono l'accesso di Kubelet al server API.

Alert	Soglie	Azione
Node High CPU	Il carico della CPU supera l'80% in un periodo di 5 minuti.	AMS determina se uno o più pod stanno consumando una quantità insolitamente elevata di CPU. Quindi, AMS verifica con te che le tue richieste, i limiti e l'attività dei pod siano quelli previsti.
Node OOM Kill rilevato	Il nodo segnala almeno un blocco OOM dell'host in una finestra di 4 minuti.	AMS determina se il kill OOM è causato dal raggiungimento del limite del contenitore o dall'overcommit del nodo. Se l'attività dell'applicazione è normale, AMS fornisce informazioni sulle richieste e sui limiti relativi agli overcommit e alla revisione dei limiti dei pod.
Node Conntrack Limit	Il rapporto tra il numero attuale di voci di tracciamento della connessione e il limite massimo supera l'80% in un periodo di 5 minuti.	AMS ti consiglia il valore di conntrack consigliato per core. I nodi Kubernetes impostano il valore massimo di conntrack proporzionalmente alla capacità di memoria totale del nodo. Le applicazioni ad alto carico, specialmente su nodi più piccoli, possono facilmente superare il valore massimo di conntrack, con conseguenti reimpostazioni e timeout della connessione.

Alert	Soglie	Azione
Node Clock non sincronizzato	Lo stato di sincronizzazione minimo in un periodo di 2 minuti è 0 e l'errore massimo in secondi è 16 o superiore.	AMS determina se il Network Time Protocol (NTP) è installato e funziona correttamente.
CPU Pod High	L'utilizzo della CPU di un container supera l'80% con una frequenza di 3 minuti per un periodo minimo di 2 minuti.	AMS analizza i log dei pod per determinare le attività dei pod che consumano una quantità elevata di CPU.
Pod High Memory	L'utilizzo della memoria di un contenitore supera l'80% del limite di memoria specificato per un periodo di 2 minuti.	AMS analizza i log dei pod per determinare le attività dei pod che consumano una quantità elevata di memoria.
CoredNS inattivo	CoredNS è scomparso da Prometheus Target Discovery per più di 15 minuti.	Si tratta di un avviso critico che indica che la risoluzione dei nomi di dominio per i servizi di cluster interni o esterni è stata interrotta. AMS controlla lo stato dei pod CoreDNS, verifica la configurazione CoreDNS, verifica gli endpoint DNS che puntano ai pod CoreDNS, verifica i limiti CoreDNS e, con l'approvazione dell'utente, abilita la registrazione del debug CoreDNS.

Alert	Soglie	Azione
Errori CoredNS	CoredNS restituisce errori SERVFAIL per oltre il 3% delle richieste DNS in un periodo di 10 minuti.	Questo avviso potrebbe segnalare un problema con un'applicazione o una configurazione errata. AMS controlla lo stato dei pod CoreDNS, verifica la configura zione CoreDNS, verifica gli endpoint DNS che puntano ai pod CoreDNS, verifica i limiti CoreDNS e, con l'approva zione dell'utente, abilita la registrazione del debug CoreDNS.
Latenza CoredNS	Il 99° percentile della durata delle richieste DNS supera i 4 secondi per 10 minuti.	Questo avviso segnala che CoredNS potrebbe essere sovraccarico. AMS controlla lo stato dei pod CoreDNS, verifica la configurazione CoreDNS, verifica gli endpoint DNS che puntano ai pod CoreDNS, verifica i limiti CoreDNS e, con l'approva zione dell'utente, abilita la registrazione del debug CoreDNS.

Alert	Soglie	Azione
Latenza di inoltro CoredNS	Il 99° percentile del tempo di risposta per le richieste di inoltro di CoredNS a kube-dns supera i 4 secondi in un periodo di 10 minuti.	Quando CoreDNS non è il server autorevole o non dispone di una voce di cache per un nome di dominio, CoreDNS inoltra la richiesta DNS a un server DNS upstream. Questo avviso segnala che CoredNS potrebbe essere sovraccar ico o che potrebbe esserci un problema con un server DNS upstream. AMS controlla lo stato dei pod CoreDNS, verifica la configurazione CoreDNS, verifica gli endpoint DNS che puntano ai pod CoreDNS, verifica i limiti CoreDNS e, con l'approva zione dell'utente, abilita la registrazione del debug CoreDNS.

Alert	Soglie	Azione
Errore di inoltro CoredNS	Oltre il 3% delle query DNS fallisce in un periodo di 5 minuti.	Quando CoreDNS non è il server autorevole o non dispone di una voce di cache per un nome di dominio, CoreDNS inoltra la richiesta DNS a un server DNS upstream. Questo avviso segnala una possibile configurazione errata o un problema con un server DNS upstream. AMS controlla lo stato dei pod CoreDNS, verifica la configurazione CoreDNS, verifica gli endpoint DNS che puntano ai pod CoreDNS, verifica i limiti CoreDNS e, con l'approva zione dell'utente, abilita la registrazione del debug CoreDNS.

Requisiti per il monitoraggio e la gestione degli incidenti per Amazon EKS in AMS Accelerate

Queste sono le risorse and/or richieste supportate per il monitoraggio e la gestione degli incidenti per Amazon EKS for AMS Accelerate

- Versioni Kubernetes supportate: consulta le versioni di Amazon EKS Kubernetes nella Guida per l'utente di Amazon EKS.
- Tipi di nodi: sono supportati i nodi gestiti di Amazon EKS. I nodi e i contenitori Windows non sono supportati.
- Accesso al cluster Kubernetes: AMS richiede il ruolo del cluster RBAC system:masters e l'utente del cluster.

- Agente SSM sui nodi Amazon EC2: sia le AMI Bottle Rocket che Amazon EKS dispongono di SSM Agent preinstallato. Assicurati che SSM Agent sia installato sulle tue AMI personalizzate e sui nodi Amazon EC2.
- Quotas di servizio Per ulteriori informazioni, consulta le quote di servizio per Amazon Managed Service for Prometheus e Amazon Managed Grafana.
- Regioni supportate: AWS

Nome Regione	Regione	Area di archiviazione delle metriche
Stati Uniti orientali (Ohio)	us-east-2	us-east-2
US East (N. Virginia)	us-east-1	us-east-1
Stati Uniti occidentali (Oregon)	us-west-2	us-west-2
Asia Pacifico (Tokyo)	ap-northeast-1	ap-northeast-1
Asia Pacifico (Seoul)	ap-northeast-2	ap-northeast-2
Asia Pacific (Singapore)	ap-southeast-1	ap-southeast-1
Asia Pacific (Sydney)	ap-southeast-2	ap-southeast-2
Europa (Francoforte)	eu-central-1	eu-central-1
Europe (Ireland)	eu-west-1	eu-west-1
Europe (London)	eu-west-2	eu-west-2
Africa (Città del Capo)	af-south-1	eu-west-1 eu-west-2
Asia Pacific (Hong Kong)	ap-east-1	ap-northeast-1 ap-northeast-2

> **Note**
>
> Le metriche per i cluster Amazon EKS in af-south-1, Africa (Città del Capo) e ap-east-1, Asia Pacifico (Hong Kong) vengono esportate rispettivamente nel servizio di monitoraggio AMS nello stesso paese. Regione AWS Le relative metriche Regioni AWS vengono quindi trasferite all'interno del servizio di monitoraggio AMS in diverse regioni, dove vengono elaborate e archiviate. Consulta la tabella precedente per le regioni utilizzate dal servizio di monitoraggio AMS per archiviare le metriche.

Integrazione al monitoraggio e alla gestione degli incidenti per Amazon EKS in AMS Accelerate

Esegui i seguenti passaggi per avviare il monitoraggio e la gestione degli incidenti per Amazon EKS.

1. Abilita i tag di ottimizzazione dei costi di Amazon EKS: consulta Tagging your resources for billing nella Amazon EKS User Guide.
2. Avvia l'onboarding del monitoraggio e della gestione degli incidenti per EKS: contatta il tuo Cloud Service Delivery Manager (CSDM) con i nomi degli account e dei cluster da inserire. IDs
3. Convalida i requisiti: il tuo Cloud Architect (CA) verifica che tutti i requisiti siano soddisfatti prima dell'inizio dell'onboarding.
4. Aggiorna il controllo degli accessi basato sui ruoli (RBAC) di Kubernetes: AMS condivide i comandi per implementare queste modifiche. `eksctl` Puoi rivedere queste modifiche e quindi distribuirle. È necessario distribuire gli aggiornamenti RBAC in modo che AMS disponga delle autorizzazioni per eseguire comandi per conto dell'utente. Questi aggiornamenti includono la mappatura del ruolo AMS IAM su un utente Kubernetes, la creazione di un nuovo ruolo del cluster Kubernetes per AMS e l'associazione del ruolo del cluster AMS Kubernetes all'utente.
5. Distribuisci i componenti del cluster: AMS distribuisce i seguenti componenti in uno spazio dei nomi gestito da AMS sul tuo cluster:
   - Server Prometheus
   - Esportatore di nodi Prometheus (non applicabile per) AWS Fargate
   - kube-state-metrics

6. Esegui gli aggiornamenti della configurazione di Prometheus: AMS configura Prometheus per abilitare la scrittura remota delle metriche.
7. (Facoltativo) Configura i dashboard: la tua CA ti aiuta a configurare i dashboard di Amazon Managed Grafana nel tuo account.

> **Note**
>
> Dopo l'onboarding del cluster Amazon EKS, AMS analizza i segnali di avviso ed esegue una valutazione di base per identificare i problemi esistenti nel cluster. Una volta completata la valutazione di base, AMS condivide i risultati e le raccomandazioni per la correzione tramite Trusted Advisor e una richiesta di assistenza che è possibile utilizzare per risolvere i problemi nel cluster. A partire dalla valutazione, AMS crea una base di monitoraggio Amazon EKS specifica per i tuoi cluster EKS regolando le nostre soglie di allarme a livello di account. Per eliminare le risposte AMS duplicate rispetto a questi risultati, modifichiamo il nostro monitoraggio per escludere tali segnali di avviso. Adattiamo nuovamente il nostro monitoraggio per includere i segnali quando il CSDM ci informa che i problemi sottostanti sono stati risolti.

Offboard dal monitoraggio e dalla gestione degli incidenti per Amazon EKS in AMS Accelerate

Informa il tuo cloud service delivery manager (CSDM) con i nomi degli account IDs e dei cluster per avviare il processo di offboarding. Dopo l'offboard, l'elaborazione degli avvisi, lo storage delle metriche e l'interrogazione dei parametri vengono sospesi e i parametri vengono eliminati in base alle politiche di conservazione dei dati predefinite di Amazon Managed Service for Prometheus.

AMS esegue le seguenti fasi di offboarding:

1. AMS disabilita gli avvisi inviati a te e ad AMS Operations.
2. AMS rimuove l'istanza Prometheus dal cluster Amazon EKS.
3. AMS rimuove altre AWS risorse installate nel tuo account, come i ruoli e le regole IAM. AWS Config

Una volta completati questi passaggi, è necessario completare i seguenti passaggi di offboarding:

1. Utilizzare `eksctl` per rimuovere le autorizzazioni RBAC di Kubernetes da. `aws-auth` `ConfigMap`
2. Se l'hai installata in precedenza, rimuovi l'istanza Amazon Managed Grafana che hai configurato per la connessione ad AMS.

Gestione della continuità in AMS Accelerate

AMS sfrutta i vantaggi AWS Backup per centralizzare e automatizzare il backup dei dati tra i servizi. AWS I piani di backup AMS forniscono le migliori pratiche per vari casi d'uso; tuttavia, siete invitati a continuare a utilizzare i piani di backup esistenti. Dopo aver aderito alla gestione dei backup di AMS, AMS fornisce report di backup e gli esperti AMS monitorano continuamente le attività di backup per garantire che disponiate di una soluzione di backup affidabile.

Per ulteriori informazioni, consulta AWS Backup: Come funziona e AWS risorse supportate e applicazioni di terze parti.

AMS Accelerate offre una gamma di servizi operativi per aiutarti a raggiungere l'eccellenza operativa su AWS. Per comprendere rapidamente come AMS aiuta i team a raggiungere l'eccellenza operativa complessiva Cloud AWS grazie ad alcune delle nostre funzionalità operative chiave, tra cui l'helpdesk 24 ore su 24, 7 giorni su 7, il monitoraggio proattivo, la sicurezza, l'applicazione di patch, la registrazione e il backup, consulta i diagrammi dell'architettura di riferimento di AMS.

Guardate il video di Carl per saperne di più (9:29)

Argomenti

- Come funziona la gestione della continuità in AMS
- Seleziona un piano di backup AMS
- Etichetta le tue risorse per applicare i piani di backup AMS
- Visualizza i backup nei vault AMS
- Monitoraggio e reportistica dei backup con AMS

Come funziona la gestione della continuità in AMS

I piani di backup AMS definiscono la frequenza di backup dei dati e la politica di conservazione dei backup. Gli archivi di backup AMS mantengono i dati di backup organizzati. Una volta associata una risorsa a un piano di backup, il backup delle risorse compatibili viene effettuato in modo incrementale. Il primo backup è una copia completa e i backup successivi acquisiscono le modifiche incrementali. A seconda della risorsa e del piano di backup AMS selezionato, Point-in-time Restore (PITR) consente di riavvolgere le risorse selezionando un momento per il ripristino. Per iniziare a usare AMS Backup Management, basta selezionare un piano di backup AMS e contrassegnare le risorse.

> **Note**
>
> Assicurati che AWS Backup sia abilitato per ogni account e tipo di risorsa seguendo i passaggi riportati qui: Guida introduttiva 1: Service Opt-in. Regione AWS
> Non è necessario continuare con Getting started 2: Create on demand backup.

Argomenti correlati di AWS Backup

- Utilizzo dei backup (creazione, modifica, copia, ripristino, eliminazione)
- Creazione di un backup on demand
- Creazione di copie di backup su Regioni AWS
- AWS Backup Servizi supportati
- Point-in-time ripristinare
- AWS Backup Caratteristiche

Seleziona un piano di backup AMS

AMS offre tre diversi piani di backup con un quarto piano di backup per ridurre al minimo i costi durante l'onboarding. Per selezionare un piano di backup AMS per ogni risorsa supportata, contrassegna la risorsa con il tag associato al piano. Durante l'accesso ad Accelerate, AMS collaborerà con voi per identificare il piano di backup più adatto alle vostre esigenze.

> **Important**
>
> Non modificate i piani di backup predefiniti di AMS, poiché le modifiche potrebbero andare perse. Crea invece nuovi piani per le tue configurazioni personalizzate. Per ulteriori informazioni, consulta Creazione di un piano di backup.

Piano di backup AMS predefinito

AWS Backup il backup continuo non è abilitato per questo piano di backup; per i dettagli, consulta Ripristino a un'ora specificata utilizzando il point-in-time ripristino (PITR).

Chiave TAG: `ams:rt:backup-orchestrator`

Valore TAG: `true`

Piano di backup AMS predefinito	Start Time	Retention
backup orario	N/D	N/D
backup giornaliero	ogni giorno 4:00 UTC	7 giorni
backup settimanale	sabato, 2:00 UTC	4 settimane
backup mensile	1° del mese, 2:00 UTC	26 settimane
backup annuale	1 gennaio, 2:00 UTC	2 anni

Piano di backup avanzato

AWS Backup il backup continuo è abilitato con la massima conservazione (31 giorni) sulle risorse supportate; per i dettagli, vedere Ripristino a un'ora specificata utilizzando il point-in-time ripristino (PITR) e Servizi e applicazioni supportati per il point-in-time ripristino (PITR).

Chiave TAG: `ams:rt:backup-orchestrator-enhanced`

Valore TAG: `true`

Piano di backup avanzato	Start Time	Retention
backup orario	N/D	N/D
backup giornaliero	ogni giorno 4:00 UTC	31 giorni
backup settimanale	sabato, 2:00 UTC	6 settimane
backup mensile	1° del mese, 2:00 UTC	26 settimane
backup annuale	1 gennaio, 2:00 UTC	2 anni

Piano di backup per dati sensibili

AWS Backup il backup continuo è abilitato con la massima conservazione (31 giorni) sulle risorse supportate; per i dettagli, vedere Ripristino a un'ora specificata utilizzando il point-in-time ripristino (PITR) e Servizi e applicazioni supportati per il point-in-time ripristino (PITR).

Chiave TAG: `ams:rt:backup-orchestrator-data-sensitive`

Valore TAG: `true`

Piano di backup per dati sensibili	Start Time	Retention
backup orario	ogni ora	7 giorni
backup giornaliero	ogni giorno 4:00 UTC	31 giorni
backup settimanale	sabato, 2:00 UTC	6 settimane
backup mensile	1° del mese, 2:00 UTC	26 settimane
backup annuale	1 gennaio, 2:00 UTC	2 anni

Piano di backup AMS Accelerate Onboarding

AWS Backup il backup continuo non è abilitato per questo piano di backup; per i dettagli, consulta Ripristino a un'ora specificata utilizzando il point-in-time ripristino (PITR).

Chiave TAG: `ams:rt:backup-orchestrator-onboarding`

Valore TAG: `true`

Piano di backup AMS Accelerate Onboarding	Start Time	Retention
backup orario	ogni ora	2 settimane
backup giornaliero	N/D	N/D
backup settimanale	N/D	N/D

Piano di backup AMS Accelerate Onboarding	Start Time	Retention
backup mensile	N/D	N/D
backup annuale	N/D	N/D

Argomenti correlati AWS Backup

- Creazione di un piano di backup
- Point-in-time restore (PITR) consente il backup continuo delle risorse supportate e consente di selezionare un momento specifico per il ripristino. Per un elenco delle risorse supportate, consulta Disponibilità delle funzionalità per risorsa.

Etichetta le tue risorse per applicare i piani di backup AMS

Per assegnare risorse a un piano di backup AMS, contrassegna la risorsa con la coppia chiave-valore del tag del piano. Puoi utilizzare AMS Resource Tagger per applicare i piani di backup AMS a un sottoinsieme delle tue risorse o a tutte le risorse supportate nel tuo account. Se desideri utilizzare un metodo alternativo per applicare tag alle tue risorse, come AWS CloudFormation o Terraform, disattiva Resource Tagger in modo che non competa con il metodo di tagging scelto. Per ulteriori informazioni, consulta Impedire a Resource Tagger di modificare le risorse.

L'esempio seguente dimostra come utilizzare Resource Tagger per applicare il piano di backup AMS predefinito alle istanze di Amazon Elastic Compute Cloud nel tuo account. Per questo piano di backup, applica la chiave e il valore del tag. `ams:rt:backup-orchestrator` `true` Per utilizzare un piano di backup diverso, modifica la chiave in modo che corrisponda al tag key del piano di backup desiderato. Per saperne di più su AMS Resource Tagger e capire come integrare il seguente profilo di riferimento con il profilo corrente (già configurato) nel tuo account Accelerate, consulta. Accelera Resource Tagger

1. Apri la AWS AppConfig console su https://console.aws.amazon.com/systems-manager/ appconfig.
2. Scegliere l'applicazione ResourceTagger.
3. Scegli la scheda Profili di configurazione, quindi scegli CustomerManagedTags
4. Scegli Crea per creare una nuova versione.
5. Scegli JSON, quindi copia e incolla il seguente oggetto JSON:

```
{
    "AWS::EC2::Instance": {
        "AccelerateBackupPlan": {
            "Enabled": true,
            "Filter": {
                "Fn::AND": [
                    {
                        "Platform": "*"
                    }
                ]
            },
            "Tags": [
                {
                    "Key": "ams:rt:backup-orchestrator",
                    "Value": "true"
                }
            ]
        }
    }
}
```

6. Scegli Crea versione di configurazione ospitata.
7. Selezionare Start deployment (Avvia distribuzione).
8. Definisci i seguenti dettagli di distribuzione:

```
Environment: AMSInfrastructure
Hosted configuration version: Select the version that you have just created.
Deployment Strategy: AMSNoBakeDeployment
```

9. Selezionare Start deployment (Avvia distribuzione). Resource Tagger contrassegna le istanze`ams:rt:backup-orchestrator: true`, assicurando che il backup delle istanze venga eseguito in conformità con il piano di backup AMS predefinito.

Visualizza i backup nei vault AMS

È possibile controllare le notifiche di backup vault a livello di singolo archivio utilizzando i tag. È possibile disattivare le notifiche per un vault specifico aggiungendo il tag `AMSNotificationOptOut` e impostando il valore su un vault specifico. `True` Per riprendere a ricevere le notifiche dal vault, rimuovi il tag.

Per visualizzare un elenco dei tuoi backup AMS, apri la console.AWS Backup Nel riquadro di navigazione, scegli Backup vault e seleziona uno degli archivi di backup AMS dalle seguenti tabelle. Nella sezione Backup, visualizza l'elenco di tutti i backup nel backup vault. Seleziona un backup da modificare, eliminare o ripristinare.

Vault per piani di Backup AMS

Nome AMS Vault	Chiave del tag del piano di backup AMS
ams-automated-backups	ams:rt:backup-orchestrator
ams-automated-enhanced-backups	ams: rt: backup-orchestrator-enhanced
ams-automated-data-sensitive-backup	am: rt: backup-orchestrator-data-sensitive
ams-onboarding-backups	ams:rt: backup-orchestrator-onboarding

Altri vault AMS

Nome AMS Vault	Descrizione
ams-manual-backups	Questo archivio contiene backup avviati manualmente creati dal documento `AWSManagedServices-StartBackupJob` SSM Automation e backup pre-patch creati da AMS Patch Automations prima dell'applicazione delle patch.
ams-custom-backups	Questo è l'archivio consigliato per i backup creati al di fuori dei piani di backup AMS.

Argomenti correlati AWS Backup

- Visualizza i backup per risorsa
- Lavorare con i backup

Monitoraggio e reportistica dei backup con AMS

> **Important**
>
> Il monitoraggio e il reporting dei backup AMS sono disponibili solo nelle regioni supportate da AMS. Questi sono Stati Uniti orientali (Virginia), Stati Uniti occidentali (California settentrionale), Stati Uniti occidentali (Oregon), Stati Uniti orientali (Ohio), Canada (Centrale), Sud America (San Paolo), UE (Irlanda), UE (Francoforte), UE (Londra), UE (Parigi), Asia Pacifico (Mumbai), Asia Pacifico (Seoul), Asia Pacifico (Singapore), Asia Pacifico (Sydney), Asia Pacifico (Asia Pacifico), Asia Pacifico (Sydney), Asia Pacifico (Mumbai), Asia Pacifico (Seoul), Asia Pacifico (Singapore), Asia Pacifico (Sydney), Asia Pacifico (Mumbai), Asia Pacifico (Seoul), Asia Pacifico (Singapore), Asia Pacifico (Sydney), Asia Pacifico (Mumbai), Asia Pacifico (Seoul), Asia Pacifico (Singapore), Asia Pacifico (Sydney) Tokyo).

AMS genera report self-service giornalieri e report mensili sulla copertura delle risorse e sullo stato dei processi di backup. I report mensili sono condivisi in Monthly Business Reviews (MBRs). Per ulteriori informazioni sui report di backup giornalieri, consulta Rapporto di backup giornaliero Rapporto .

Gli esperti AMS monitorano tutte le attività di backup configurate utilizzando AWS Backup. In caso di errori di backup, AMS indaga sull'errore e comunica all'utente la causa principale e le opzioni di riparazione, se disponibili. Per evitare rumori di allarme, durante gli eventi che causano un numero elevato di errori di backup negli account, AMS formula una raccomandazione collettiva, tramite il CSDM, anziché notificarvi ogni singolo errore.

Tieni presente che AMS non monitora alcun backup configurato utilizzando la funzionalità di backup autonoma di un AWS servizio.

Comprendi la gestione delle patch in AMS Accelerate

Important

Accelerate Patch Reporting implementa periodicamente una policy basata sulle AWS Glue risorse. Tieni presente che gli aggiornamenti AMS al sistema di patching sovrascrivono le politiche esistenti basate sulle risorse. AWS Glue

Important

È possibile specificare repository di patch alternativi per i nodi gestiti. Sebbene AMS implementi le configurazioni di patch richieste, l'utente è responsabile della selezione e della convalida della sicurezza dei repository scelti. È inoltre necessario accettare tutti i rischi derivanti dall'utilizzo di questi archivi, come i rischi della catena di approvvigionamento.
Di seguito sono riportate le migliori pratiche per la sicurezza del processo di gestione delle patch:

- Utilizzate solo fonti di repository affidabili e verificate
- L'impostazione predefinita è costituita dagli archivi standard dei fornitori di sistemi operativi, quando possibile
- Controlla regolarmente le configurazioni dei repository personalizzati

Puoi utilizzare il sistema di patching di AMS Accelerate, Patch Add-On, per applicare patch alle istanze con aggiornamenti relativi alla sicurezza e di altro tipo. Accelerate Patch Add-On è una funzionalità che fornisce patch basate su tag per le istanze AMS. Sfrutta la funzionalità AWS Systems Manager (SSM) in modo da poter etichettare le istanze e applicare le patch a tali istanze utilizzando una linea di base e una finestra configurate dall'utente. L'AMS Accelerate Patch Add-On è un'opzione di onboarding. Se non l'hai ottenuto durante l'onboarding del tuo account Accelerate, contatta il tuo cloud service delivery manager (CSDM) per richiederlo.

La gestione delle patch di AMS Accelerate utilizza la funzionalità di base delle patch di Systems Manager per controllare la definizione delle patch applicate su un'istanza. La patch baseline contiene l'elenco delle patch preapprovate, ad esempio tutte le patch di sicurezza. La conformità dell'istanza

viene misurata rispetto alla linea di base della patch ad essa associata. AMS Accelerate, per impostazione predefinita, installa tutte le patch disponibili per mantenere l'istanza aggiornata.

> **Note**
>
> AMS Accelerate applica solo le patch del sistema operativo (OS). Ad esempio, per Windows, vengono applicati solo gli aggiornamenti di Windows, non gli aggiornamenti di Microsoft.

Per informazioni sui report, vedereRapporti sulla gestione degli host AMS.

AMS Accelerate offre una gamma di servizi operativi per aiutarti a raggiungere l'eccellenza operativa su AWS. Per comprendere rapidamente come AMS aiuta i team a raggiungere l'eccellenza operativa complessiva Cloud AWS grazie ad alcune delle nostre funzionalità operative chiave, tra cui l'helpdesk 24 ore su 24, 7 giorni su 7, il monitoraggio proattivo, la sicurezza, l'applicazione di patch, la registrazione e il backup, consulta i diagrammi dell'architettura di riferimento di AMS.

Argomenti

- Consigli per l'applicazione delle patch
- Creare una finestra di manutenzione delle patch in AMS
- Toppa con ganci
- Linea base delle patch AMS Accelerate
- Creazione di un ruolo IAM per l'applicazione di patch su richiesta di AMS Accelerate
- Comprendi le notifiche e gli errori delle patch in AMS Accelerate

Consigli per l'applicazione delle patch

Se ti occupi di operazioni applicative o infrastrutturali, comprendi l'importanza di una soluzione di patching del sistema operativo (OS) sufficientemente flessibile e scalabile da soddisfare i diversi requisiti dei tuoi team applicativi. In un'organizzazione tipica, alcuni team applicativi utilizzano un'architettura che prevede istanze immutabili, mentre altri distribuiscono le proprie applicazioni su istanze mutabili.

Per ulteriori informazioni sulla guida AWS prescrittiva per l'applicazione di patch, consulta Applicazione automatica delle patch per istanze mutabili nell'utilizzo del cloud ibrido. AWS Systems Manager

> **Note**
>
> Accelerate Patch Add-On è una funzionalità che fornisce patch basate su tag per le istanze AMS. Sfrutta la funzionalità AWS Systems Manager (SSM) in modo da poter etichettare le istanze e applicare le patch a tali istanze utilizzando una linea di base e una finestra configurate dall'utente. L'AMS Accelerate Patch Add-On è un'opzione di onboarding. Se non l'hai ottenuto durante l'onboarding del tuo account Accelerate, contatta il tuo cloud service delivery manager (CSDM) per richiederlo.

Consigli sulla responsabilità delle patch

Il processo di applicazione delle patch per le istanze persistenti dovrebbe coinvolgere i seguenti team e le seguenti azioni:

- I team applicativi (DevOps) definiscono i gruppi di patch per i propri server in base all'ambiente applicativo, al tipo di sistema operativo o ad altri criteri. Definiscono inoltre le finestre di manutenzione specifiche per ciascun gruppo di patch. Queste informazioni devono essere memorizzate nei tag allegati alle istanze. I nomi di tag consigliati sono «Patch Group» e «Maintenance Window». Durante ogni ciclo di patch, i team applicativi si preparano all'applicazione delle patch, testano l'applicazione dopo l'applicazione e risolvono eventuali problemi relativi alle applicazioni e al sistema operativo durante l'applicazione.
- Il team addetto alle operazioni di sicurezza definisce le linee di base delle patch per vari tipi di sistema operativo utilizzate dai team delle applicazioni e rende le patch disponibili tramite Systems Manager Patch Manager.
- La soluzione di patching automatizzata viene eseguita regolarmente e distribuisce le patch definite nelle patch baseline, in base ai gruppi di patch e alle finestre di manutenzione definiti dall'utente.
- I team di governance e conformità definiscono le linee guida per l'applicazione delle patch e i processi e i meccanismi di eccezione.

Per ulteriori informazioni, consulta Progettazione di soluzioni di patching per istanze EC2 mutabili.

Linee guida per i team applicativi

- Rivedi e acquisisci familiarità con la creazione e la gestione delle finestre di manutenzione; consulta Finestre di AWS Systems Manager manutenzione e Creazione di una finestra di

manutenzione SSM per l'applicazione delle patch per saperne di più. Comprendere la struttura generale e l'uso delle finestre di manutenzione ti aiuta a capire quali informazioni fornire se non sei tu a crearle.

- Per le configurazioni High Availability (HA), si prevede di avere una finestra di manutenzione per zona di disponibilità e per ambiente (Dev/Test/Prod). Ciò garantirà la disponibilità continua durante l'applicazione delle patch.
- La durata della finestra di manutenzione consigliata è di 4 ore con un limite di 1 ora, più 1 ora aggiuntiva ogni 50 istanze
- Applicate le patch Dev e Test con un intervallo di tempo sufficiente tra una e l'altra per consentire di identificare eventuali problemi prima dell'applicazione delle patch di produzione.
- Automatizzate le attività più comuni precedenti e successive all'applicazione delle patch tramite l'automazione SSM ed eseguitele come attività della finestra di manutenzione. Tieni presente che per le attività successive all'applicazione delle patch devi assicurarti che sia assegnato un tempo sufficiente, poiché le attività non verranno avviate una volta raggiunto il limite.
- Acquisisci familiarità con le Patch Baseline e le relative funzionalità, in particolare per quanto riguarda i ritardi di approvazione automatica per i tipi di gravità delle patch, che possono essere utilizzati per garantire che solo le patch applicate Dev/Test vengano applicate in produzione in un secondo momento. Per ulteriori dettagli, consulta Informazioni sulle linee di base delle patch.

Guida per i team addetti alle operazioni di sicurezza

- Rivedi e acquisisci familiarità con le linee di base delle patch. L'approvazione delle patch viene gestita in modo automatizzato e prevede diverse opzioni di regole. Per ulteriori informazioni, consulta Informazioni sulle linee di base delle patch.
- Discutete le esigenze relative all'applicazione delle patch Dev/Test/Prod con i team delle applicazioni e sviluppate più linee di base per soddisfare queste esigenze.

Linee guida per i team di governance e conformità

- L'applicazione delle patch dovrebbe essere una funzione di «Opt Out». Dovrebbero esistere una finestra di manutenzione predefinita e un'etichettatura automatica per garantire che nulla rimanga senza patch. AMS Resource Tagger può aiutarti in questo senso; discuti di questa opzione con il tuo cloud architect (CA) o il cloud service delivery manager (CSDM) per ricevere indicazioni sull'implementazione.

- Le richieste di esenzione dall'applicazione di patch dovrebbero richiedere la documentazione che giustifichi l'esenzione. Un Chief Information Security Officer (CISO) o altro responsabile dell'approvazione dovrebbe approvare o rifiutare la richiesta.
- La conformità delle patch deve essere verificata regolarmente tramite la console Patch Manager, Security Hub o uno scanner di vulnerabilità.

Esempio di progettazione per un'applicazione Windows ad alta disponibilità

Panoramica:

- Una finestra di manutenzione per AZ.
- Un set di finestre di manutenzione per ambiente.
- Una patch di base per ambiente:
  - Sviluppo: approva tutta la severità e la classificazione dopo 0 giorni.
  - Test: approva le patch di aggiornamento di sicurezza critiche dopo 0 giorni e tutte le altre classificazioni e livelli di gravità dopo 7 giorni.
  - Prodotto: Approva le patch di aggiornamento fondamentali per la sicurezza dopo 0 giorni e tutte le altre classificazioni e livelli di gravità dopo 14 giorni.

CloudFormation Script:

Questi script sono configurati per creare le finestre di manutenzione, le linee di base e le attività di applicazione delle patch per un'applicazione Windows HA EC2 con due zone di disponibilità utilizzando le impostazioni di approvazione di base sopra descritte.

- Esempio di stack CFN per Windows Dev: HA-Patching-dev-Stack.json
- Esempio di stack CFN di Windows Test: HA-Patching-Test-Stack.json
- Esempio di stack CFN per Windows Prod: HA-Patching-Prod-Stack.json

Consigli sulle patch FAQs

D: Come si gestiscono le patch non pianificate per gli exploit che durano «0" giorni?

R: SSM supporta una funzionalità Patch Now che utilizza la linea di base predefinita corrente per il sistema operativo dell'istanza. AMS implementa un set predefinito di Patch Baseline che approva tutte le patch dopo 0 giorni. Tuttavia, quando si utilizza la funzionalità Patch Now, non viene eseguita un'istantanea prima della patch, poiché questo comando esegue il documento AWS-RunPatchBaseline SSM. Ti consigliamo di eseguire un backup manuale prima di applicare le patch.

D: AMS supporta l'applicazione di patch per le istanze in Auto-Scaling Groups ()? ASGs

R: No. Al momento, l'applicazione di patch ASG non è supportata per i clienti Accelerate.

D: Esistono limitazioni da tenere a mente per Maintenance Windows?

R: Sì, ci sono alcune limitazioni di cui dovresti essere a conoscenza.

- Windows di manutenzione per account: 50
- Attività per finestra di manutenzione: 20
- Numero massimo di automazioni simultanee per finestra di manutenzione: 20
- Numero massimo di finestre di manutenzione simultanee: 5

Per un elenco completo dei limiti SSM predefiniti, consulta AWS Systems Manager endpoint e quote.

Creare una finestra di manutenzione delle patch in AMS

Una finestra di manutenzione delle patch esegue le automazioni delle patch AMS secondo una pianificazione prestabilita per EC2 istanze Amazon mirate. Gli obiettivi sono definiti da uno o più tag per un gruppo di istanze. Puoi impostare pianificazioni in base ai giorni e agli orari intorno al Patch Tuesday oppure puoi definire una pianificazione utilizzando un'espressione cron. Per ulteriori informazioni, vedere Reference: Cron and rate expressions for Systems Manager nella Guida per l'AWS Systems Manager utente. Prima dell'applicazione delle patch, AMS crea un'istantanea del volume root di ogni istanza. Se AMS rileva che l'applicazione delle patch influisce sullo stato dell'istanza o se notifichi ad AMS l'impatto dell'applicazione derivante dall'applicazione delle patch, AMS utilizza questa istantanea per ripristinare il volume root allo stato precedente alla patch.

Limiti della finestra di manutenzione delle patch di AMS Accel

L'applicazione di patch AMS utilizza AWS Systems Manager (Systems Manager). Oltre ai limiti del servizio Systems Manager, l'applicazione delle patch con AMS ha un limite di 300 istanze di

destinazione per finestra di manutenzione delle patch. Dato un tempo generale di completamento delle patch di 30 minuti per istanza, la tabella seguente fornisce esempi di numero di finestre e durate di manutenzione.

Istanze da correggere	Durata delle finestre di manutenzione (ore)	Sono necessarie finestre di manutenzione concomitanti
100	1	1
200	1	1
300	2	1
600	3	2
800	4	3
1200	6	4
1500	8	5

> **Important**
>
> Questi esempi presuppongono che non siano attive altre finestre di manutenzione di Systems Manager e che non siano in esecuzione altre automazioni.

Per ulteriori informazioni sui limiti, consulta AWS Systems Manager endpoint e quote.

Argomenti

- Crea una finestra di manutenzione ricorrente «Patch Tuesday» dalla console AMS (consigliato)
- Crea una finestra di manutenzione delle patch utilizzando CloudFormation AMS Accelerate
- Creare una finestra di manutenzione dalla console Systems Manager per AMS Accelerate
- Crea una finestra di manutenzione con l'interfaccia a riga di comando (CLI) di Systems Manager per AMS Accelerate

Crea una finestra di manutenzione ricorrente «Patch Tuesday» dalla console AMS (consigliato)

Microsoft rilascia le patch per i suoi sistemi operativi il secondo martedì di ogni mese, noto anche come Patch Tuesday. È comune pianificare l'applicazione delle patch per le istanze Windows e Linux in relazione al Patch Tuesday. Per pianificare le finestre ricorrenti di manutenzione delle patch nel primo o nel secondo fine settimana dopo Patch Tuesday, visita la console AMS e segui questi passaggi:

1. Fornisci un nome per la finestra di manutenzione delle patch.
2. [opzionale] Fornisci una descrizione per la finestra di manutenzione delle patch.
3. Seleziona un giorno relativo al Patch Tuesday.
4. Inserisci l'ora di inizio della finestra di manutenzione della patch in hh:mm. Ad esempio, mezzanotte è 00:00 e le 23:00 sono 23:00. Quindi seleziona un fuso orario.
5. [opzionale] Modifica la durata in base alle tue esigenze. AMS consiglia una durata minima di quattro ore.
6. Inserisci la chiave e il valore del tag di patch per l'obiettivo. Per informazioni, consulta Cosa sono i tag? .
7. [opzionale] Espandi i parametri opzionali per regolare la concorrenza, il tasso di errore e la chiusura degli intervalli di manutenzione.

    1. La concorrenza controlla quante istanze di destinazione stanno applicando le patch contemporaneamente. Ad esempio, una concorrenza del 50% per 10 istanze di destinazione applicherà le patch a non più di 5 istanze alla volta, mentre una concorrenza del 100% applicherà le patch a tutte e 10 contemporaneamente.
    2. Il tasso di errore controlla la tolleranza agli errori prima che l'applicazione delle patch venga sospesa. Ad esempio, un tasso di errore del 100% per 10 istanze di destinazione applicherà la patch a tutte le istanze indipendentemente dal numero di errori, mentre un tasso di errore del 50% sospenderà l'applicazione delle patch una volta che 5 istanze non sono riuscite a eseguire la patch. AMS consiglia un tasso di errore del 100%.
    3. L'interruzione della finestra di manutenzione delle patch previene la violazione della finestra di manutenzione delle patch sospendendo l'inizio di nuove attività di patch nelle ore specificate prima della fine della finestra di manutenzione delle patch. Ad esempio, un intervallo di 1 ora (consigliato) interrompe le nuove attività relative alle patch 1 ora prima della fine della finestra di manutenzione delle patch.

> **Important**
>
> Verifica l'ora di esecuzione successiva.
> Visita la console SSM Maintenance Window, cerca la finestra di manutenzione delle patch appena creata e verifica l'ora di esecuzione successiva. Se hai domande o devi modificare la finestra di manutenzione delle patch, crea una richiesta di assistenza per parlare con un esperto di patch AMS

Per pianificare una finestra di manutenzione delle patch basata su CRON utilizzando CloudFormation, vediCrea una finestra di manutenzione delle patch utilizzando CloudFormation AMS Accelerate.

Crea una finestra di manutenzione delle patch utilizzando CloudFormation AMS Accelerate

Per creare una finestra di manutenzione delle patch di AMS Accelerate utilizzando AWS CloudFormation, accedi prima al tuo account Accelerate e seleziona Regione AWS dove risiedono le istanze di destinazione. Quindi segui questi passaggi su /cloudformation: https://console.aws.amazon.com

1. Seleziona uno dei due modelli di patching Accelerate personalizzati. CloudFormation

   - Pianificazione del Patch Tuesday: Microsoft rilascia le patch per i suoi sistemi operativi il secondo martedì di ogni mese, noto anche come Patch Tuesday, per pianificare le finestre di manutenzione delle patch il primo o il secondo fine settimana dopo Patch Tuesday: Una volta effettuato l'accesso alla console Accelerate, usa questo modello di collegamento. PatchTuesdayScheduling CloudFormation
   - Pianificazione CRON: per creare finestre di manutenzione delle patch utilizzando CRON per definire il giorno di inizio, usa questo modello di link. CRONScheduling CloudFormation Ricorda che Systems Manager CRON conta i giorni da 1 a 7 (per i dettagli su Systems Manager CRON, vedi Riferimento: Cron and rate expressions for Systems Manager).

   La scelta di uno di questi collegamenti causa il caricamento automatico del modello sulla console. CloudFormation Fai clic su Next (Successivo).
2. Nella pagina Specificare i dettagli dello stack (passaggio 2 delle pagine Create Stack), inserisci il nome dello stack e i parametri del modello (i parametri predefiniti mostrati sono quelli predefiniti

consigliati da AMS, seleziona il giorno e l'ora in base al tuo caso d'uso). Al termine, fai clic su Avanti.

3. Configura le opzioni dello stack (opzionale). Per informazioni sulle opzioni, consulta Setting AWS CloudFormation stack options. Al termine, fai clic su Avanti.
4. Controlla i valori dello stack (facoltativo). Per informazioni sulla revisione dei dettagli dello stack per stimare i costi, consulta Revisione dello stack e stima del costo dello stack. Quando sei pronto, fai clic su Crea pila.

   La creazione dello stack può richiedere fino a un minuto. Una volta creato correttamente lo stack, la finestra di manutenzione delle patch viene eseguita all'ora specificata. È possibile apportare modifiche alla finestra di manutenzione delle patch creando ed eseguendo un set di CloudFormation modifiche (consigliato) (per ulteriori informazioni, vedere Creazione di stack utilizzando i changeset) o aggiornando la finestra di manutenzione delle patch sulla console della finestra di manutenzione di Systems Manager (). https://console.aws.amazon.com/systems-manager/maintenance-windows

Guardate il video di Namrata per saperne di più (5:41)

Creare una finestra di manutenzione dalla console Systems Manager per AMS Accelerate

Per creare una finestra di manutenzione di AMS Accelerate dalla console Systems Manager, procedi nel seguente modo:

1. Nella barra di navigazione a sinistra dell'area di gestione delle modifiche, fai clic su Finestre di manutenzione, quindi su Crea finestra di manutenzione in alto a destra dello schermo. Compila il modulo. Per i dettagli su una qualsiasi delle opzioni, consulta Creare una finestra di manutenzione (console). Al termine, fai clic su Crea finestra di manutenzione.

   Viene visualizzata la pagina con l'elenco delle finestre di manutenzione.
2. Seleziona la finestra di manutenzione appena creata.

   Si apre la pagina dei dettagli della finestra di manutenzione.
3. Vai alla scheda Obiettivi e scegli Registra obiettivo.

   Viene visualizzata la pagina Registra obiettivo.

4. Aggiungi il tuo obiettivo Accelerate. Per informazioni sugli obiettivi, consulta Assegnare gli obiettivi a una finestra di manutenzione (console). Al termine, fai clic su Registra obiettivo. Prendi nota dell'obiettivo quando ne avrai bisogno in seguito.

   La pagina dei dettagli delle finestre di manutenzione si riapre nella scheda Obiettivi con un elenco che include il nuovo obiettivo.

5. Nella scheda Attività della pagina dei dettagli della finestra di manutenzione, scegli Registra attività, quindi seleziona Registra attività di automazione dall'elenco a discesa. Compila il modulo. Accelera le note:

   - Fornisci un nome significativo per l'attività. Ad esempio: AcceleratePatch.
   - Nell'area del documento di automazione, fai clic sulla casella di ricerca, scegli Proprietario, quindi Documenti condivisi.
   - Seleziona il documento di automazione facendo clic nella casella di ricerca e scegliendo Prefisso del nome del documento --> Uguale a, quindi digitando:. AWSManagedServices-PatchInstance Quindi seleziona il AWSManagedServices-PatchInstancedocumento selezionando il relativo pulsante di opzione.
   - In Versione del documento, scegli Versione predefinita in fase di esecuzione.
   - Nella sezione Obiettivi:
     - Imposta Target by: a Selezione di gruppi target registrati.
     - Nell'elenco degli obiettivi, seleziona l'obiettivo che hai registrato nella scheda Target.
   - Nella sezione Parametri di input, compila il modulo.
     - InstanceId: `{{TARGET_ID}}`
     - StartInactiveInstances: `True` per avviare le istanze se vengono interrotte durante la finestra di manutenzione della patch.

     > **Note**
     >
     > Il valore del InstanceIdparametro fa distinzione tra maiuscole e minuscole e il valore del StartInactiveInstancesparametro può essere vero o falso.
     > Le istanze interrotte non possono essere avviate quando sono indirizzate dai tag. Per ulteriori informazioni, consulta Nessuna chiamata da eseguire.

   - Nella sezione Controllo della frequenza, scegli le percentuali. AMS Accelerate consiglia il 100% per la concorrenza e il 100% per la soglia di errore per tentare di applicare patch a tutte le istanze contemporaneamente, indipendentemente dagli errori di automazione. Se desideri

applicare patch a metà degli obiettivi alla volta, ad esempio, per mantenere metà delle istanze di destinazione con un bilanciamento del carico in esecuzione, imposta Concurrency al 50%.

- Nella sezione IAM service role, seleziona Usa un ruolo di servizio personalizzato, quindi scegli ams_ssm_automation_role.

Fai clic su Registra attività di automazione.

Viene creata la finestra di manutenzione delle patch. Nella scheda Descrizione, puoi vedere l'ora di esecuzione successiva.

Crea una finestra di manutenzione con l'interfaccia a riga di comando (CLI) di Systems Manager per AMS Accelerate

Per creare una finestra di manutenzione di AMS Accelerate con l'interfaccia a riga di comando:

1. Segui il tutorial SSM: crea e configura una finestra di manutenzione (AWS CLI). Per ogni fase del tutorial, ecco alcuni esempi di comandi CLI per l'applicazione delle patch.

> **Note**
>
> Questi esempi sono specifici per Linux o macOS. I comandi possono anche essere eseguiti, il AWS CloudShell che può essere più semplice rispetto alla configurazione `awscli` su un computer locale. Per i dettagli, consulta Lavorare con. AWS CloudShell

   a. Nel passaggio 1 del tutorial, per creare una finestra di manutenzione:

```
aws ssm create-maintenance-window \
                --name Sample-Maintenance-Window \
                --schedule "cron(0 30 23 ? * TUE#2 *)" \
                --duration 4 \
                --cutoff 1 \
                --allow-unassociated-targets \
                --tags "Key=Environment,Value=Production"
```

   Se completato con successo, `window-id` viene restituito.

   b. Nella fase 2 del tutorial, per registrare un nodo di destinazione:

```
aws ssm register-target-with-maintenance-window \
                --window-id "mw-xxxxxxxxx" \
                --resource-type "INSTANCE" \
                --target "Key=tag:Environment,Values=Prod"
```

Una volta completato con successo, vengono restituiti `WindowTargetID` i messaggi.

c. Nella fase 3 del tutorial, per registrare un'attività:

```
aws ssm register-task-with-maintenance-window \
    --window-id "mw-xxxxxx" \
    --targets "Key=WindowTargetIds,Values=63d4f63c-xxxxxx-9b1d-xxxxxfff" \
    --task-arn "AWSManagedServices-PatchInstance" \
    --service-role-arn "arn:aws:iam::AWS-Account-ID:role/ams_ssm_automation_role"
 \
    --task-invocation-parameters "{\"Automation\":{\"DocumentVersion\":\"\$DEFAULT
\",\"Parameters\":{\"InstanceId\":[\"{{TARGET_ID}}\"],\"StartInactiveInstances\":
[\"True\"]}}}" \
    --max-concurrency 50 \
    --max-errors 50 \
    --name "AutomationExample" \
    --description "Sample Description" \
    --task-type=AUTOMATION
```

Toppa con ganci

È possibile configurare le patch AMS per eseguire comandi a livello di sistema operativo (OS) prima e dopo l'applicazione delle patch, utilizzando gli hook di patch AMS. Utilizza gli hook di patch AMS per eseguire i documenti di comando SSM per interrompere un servizio prima dell'applicazione delle patch e quindi avviare il servizio dopo l'applicazione delle patch, oppure per eseguire comandi per confermare che l'applicazione sia integra dopo l'applicazione.

Per utilizzare gli hook di patch AMS, devi fare quanto segue:

1. Crea documenti di comando SSM da utilizzare come patch hook.
2. Crea una finestra di manutenzione delle patch AMS o utilizza una finestra di manutenzione delle patch AMS esistente. Per i dettagli, consulta la finestra di manutenzione delle patch AMS.
3. Configura una finestra di manutenzione delle patch AMS per utilizzare i documenti del comando SSM per gli hook di patch AMS.

Agganci di patch AMS RACI

La matrice responsabile, responsabile, consultata e informata, o RACI, assegna la responsabilità principale al cliente o ad AMS per una serie di attività. La tabella seguente fornisce una panoramica delle responsabilità del cliente e di AMS per le attività in un'applicazione che utilizza patch hook AMS.

- R sta per la parte responsabile che svolge il lavoro per raggiungere l'obiettivo
- A sta per la parte responsabile
- C sta per consultata; la parte i cui pareri vengono richiesti, di solito in qualità di esperti in materia, e con la quale esiste una comunicazione bilaterale
- I sta per informato; la parte che viene informata sui progressi, spesso solo al completamento del compito o del risultato

Attività	Customer	AMS
Crea il contenuto del documento e del documento del comando SSM della pre/post patch	R	C
Configura i parametri del patch hook per l'applicazione delle patch ad AMS	R	C
Esegui il documento di comando SSM della pre/post patch	I	R
Valuta e rispondi agli errori del patch hook	I	R
Informate il cliente in caso di guasto del patch hook	I	R
Ripristina lo stato precedent e alla patch se richiesto dal cliente	C	R

Crea documenti SSM per i patch hook

I patch hook AMS utilizzano i documenti Amazon EC2 Systems Manager (SSM) durante l'applicazione delle patch. Crea un documento di comando SSM o condividi un documento di comando SSM esistente con l'account a cui viene applicata la patch. Per informazioni sui documenti SSM, incluse le limitazioni, consulta Condivisione di documenti SSM.

Per creare un documento di comando SSM, segui questi passaggi:

1. Crea un documento SSM con Document Type = «Command».
2. Inserisci i tuoi comandi nella sezione Contenuto. Per ulteriori informazioni, consulta Creazione del contenuto di un documento SSM.

> **Note**
>
> I documenti SSM per i patch hook AMS possono essere creati anche con o. AWS CLI CloudFormation Se hai bisogno di assistenza nella creazione di documenti SSM per i tuoi patch hook AMS, contatta il tuo Cloud Architect.

Configura la finestra di manutenzione delle patch AMS per utilizzare i documenti del comando SSM come patch hook AMS

Una finestra di manutenzione delle patch AMS è una finestra di manutenzione di Systems Manager che esegue l'automazione delle patch AMS configurata.

Per modificare una finestra di manutenzione delle patch AMS in modo da utilizzare i patch hook, procedi nel seguente modo:

1. Nella https://console.aws.amazon.com/systems-manager/sezione Strumenti di gestione delle modifiche nel riquadro di navigazione a sinistra, seleziona Windows di manutenzione.

   Si apre una pagina che elenca le finestre di manutenzione esistenti.
2. Seleziona un ID di finestra che inizi con mw-.

   Si apre la pagina dei dettagli per quella finestra di manutenzione.
3. Selezionate la scheda Attività e l'ID attività della finestra con l'ARN dell'operazione di AMS-PatchInstance e fate clic su Modifica.

4. Scorri verso il basso fino alla sezione Parametri e aggiorna i seguenti parametri.

Parametri del patch hook AMS:

- PrePatchHook: il nome del documento SSM di tipo «Comando» che si desidera eseguire prima dell'applicazione delle patch. Lascia questo campo vuoto o digita «AWS-noop» (con distinzione tra maiuscole e minuscole) se non stai eseguendo un comando prima dell'applicazione della patch.
- PostPatchHook: Il nome del documento SSM di tipo «Comando» che desideri eseguire dopo l'applicazione della patch. Lascia questo campo vuoto o digita «AWS-noop» (con distinzione tra maiuscole e minuscole) se non stai eseguendo un comando dopo l'applicazione della patch.
- ExecutePatchBasedOnPreHookStatus: Esegui l'applicazione delle patch in base all'esito positivo o negativo dell'esecuzione, scegline uno: PrePatchHook
  - OnPreHookSuccess: Esegui l'automazione delle patch AMS solo quando ha esito positivo. PrePatchHook
  - Sempre: esegui l'automazione delle PrePatchHook patch AMS quando ha successo e quando fallisce.
  - OnPreHookFailure- Esegui l'automazione delle patch AMS solo in caso di PrePatchHook errore.
  - Mai: non eseguire l'automazione delle patch AMS. Questo può essere utile per testare il tuo PrePatchHook.
- ExecutePostHookBasedOnPatchStatus: Esegui l'hook post-patch in base al successo o al fallimento dell'automazione delle patch AMS, scegline uno:
  - OnPatchSuccess: eseguilo solo PostPatchHook quando l'automazione delle patch AMS viene eseguita correttamente.
  - Sempre: eseguilo PostPatchHook quando l'automazione delle patch AMS ha successo e quando fallisce.
  - OnPatchFailure- Eseguilo PostPatchHook solo quando l'automazione delle patch AMS fallisce.

> **Note**
>
> Se a una di queste variabili manca la relativa casella di testo, rimediate scorrendo verso l'alto fino alla sezione del documento di automazione sulla stessa pagina e selezionando un

documento diverso, quindi riselezionando il documento originale. Ciò aggiorna i parametri di input in modo da poterli modificare.

Linea base delle patch AMS Accelerate

Una base di confronto delle patch definisce le patch approvate per essere installate nelle tue istanze. È possibile specificare singolarmente le patch approvate o rifiutate. È possibile anche creare regole di approvazione automatica per specificare che determinati tipi di aggiornamenti (ad esempio, quelli critici) devono essere approvati automaticamente. L'elenco dei rifiutati ha la priorità sulle regole e sull'elenco di quelli approvati.

Linea di base della patch predefinita

Quando si effettua l'accesso alle patch di AMS Accelerate, le linee di base delle patch predefinite vengono sostituite dalle linee di base delle patch predefinite di AMS Accelerate per i seguenti sistemi operativi.

- Windows
- Amazon Linux 1
- Amazon Linux 2
- CentOS
- Suse
- Rhel
- Ubuntu

Important

Le linee di base delle patch predefinite sono gestite da AMS. Non modificate le linee di base delle patch predefinite poiché le modifiche potrebbero andare perse. Create invece una linea di base di patch personalizzata. Per informazioni, consultare Patch di base personalizzate con AMS Accelerate.

> **Note**
>
> Le linee di base delle patch di AMS Accelerate definite come product = * indicano che tutte le patch vengono applicate all'istanza di tutte le classificazioni e di sicurezza.

Patch di base personalizzate con AMS Accelerate

Per utilizzare una linea di base di patch personalizzata con AMS Accelerate, assicurati innanzitutto di disporre di un gruppo di patch, quindi crea la baseline personalizzata.

Per ulteriori informazioni, consulta le seguenti risorse:

- Lavorare con i gruppi di patch
- Creazione di una linea di base di patch personalizzata (Windows)
- Creazione di una linea di base di patch personalizzata (Linux)
- Aggiornamento o eliminazione di una baseline di patch personalizzata (console)

Creazione di un ruolo IAM per l'applicazione di patch su richiesta di AMS Accelerate

Dopo aver effettuato l'onboarding dell'account su AMS Accelerate patching, AMS Accelerate implementa una policy gestita, amspatchmanagedpolicy. Questa policy contiene le autorizzazioni necessarie per l'applicazione di patch su richiesta utilizzando il documento di automazione AMS. `AWSManagedServices-PatchInstance` Per utilizzare questo documento di automazione, l'amministratore dell'account crea un ruolo IAM per gli utenti. Completare la procedura riportata di seguito.

Crea un ruolo utilizzando Console di gestione AWS:

1. Accedi Console di gestione AWS e apri la console IAM.
2. Nel pannello di navigazione della console, scegli Ruoli, quindi Crea ruolo.
3. Scegli un altro tipo di Account AWS ruolo.
4. Per Account ID, inserisci l'ID AWS dell'account a cui desideri concedere l'accesso alle tue risorse.

   L'amministratore dell'account specificato può concedere l'autorizzazione di assumere questo ruolo a qualsiasi utente IAM in tale account. A tale scopo, l'amministratore attribuisce all'utente o al

gruppo una politica che concede l'autorizzazione per l'azione sts: AssumeRole. Tale policy deve specificare l'Amazon Resource Name (ARN) del ruolo come risorsa. Tieni presente quanto segue:

- Se concedi le autorizzazioni agli utenti di un account che non controlli e gli utenti assumeranno questo ruolo a livello di codice, scegli Richiedi ID esterno. L'ID esterno può essere qualsiasi parola o numero concordato tra l'utente e l'amministratore dell'account di terze parti. Questa opzione aggiunge automaticamente una condizione alla politica di fiducia che consente all'utente di assumere il ruolo solo se la richiesta include il valore STS:ExternalID corretto. Per ulteriori informazioni, vedi Come utilizzare un ID esterno per concedere l'accesso alle tue AWS risorse a terzi.
- Se desideri limitare il ruolo agli utenti che accedono con l'autenticazione a più fattori (MFA), scegli Richiedi MFA. Questa opzione aggiunge una condizione alla policy di affidabilità del ruolo che controlla un accesso MFA. Gli utenti che desidera assumere il ruolo deve effettuare l'accesso temporaneo con una password una tantum temporanea configurata da un dispositivo MFA. Gli utenti senza autenticazione MFA non possono assumere il ruolo. Per ulteriori informazioni sulla MFA, vedere Utilizzo dell'autenticazione a più fattori (MFA) in. AWS

5. Scegli Successivo: autorizzazioni.

   IAM include un elenco di politiche nell'account. In Aggiungi autorizzazioni, inserisci amspatchmanagedpolicy nella casella del filtro e seleziona la casella di controllo per questa politica di autorizzazioni. Fai clic su Next (Successivo).

6. In Dettagli del ruolo, inserisci il nome del ruolo PatchRole, ad esempio aggiungi una descrizione del ruolo (consigliato), aggiungi anche tag per aiutarti a identificare questo ruolo. I nomi dei ruoli non fanno distinzione tra maiuscole e minuscole, ma devono essere univoci all'interno di Account AWS. Al termine, fai clic su Crea ruolo.

> **Note**
>
> I nomi dei ruoli non possono essere modificati dopo la loro creazione.

Comprendi le notifiche e gli errori delle patch in AMS Accelerate

> **Important**
>
> A partire dal 1° febbraio 2025, i clienti AMS non riceveranno più notifiche per le finestre vuote di Patch Maintenance nei loro account gestiti.

Richieste di assistenza patch e notifiche via e-mail

AMS crea una nuova richiesta di assistenza quattro giorni prima della successiva finestra di manutenzione delle patch. Ad esempio, quattro giorni prima dell'esecuzione di una finestra di manutenzione delle patch denominata App1 PROD, AMS crea una richiesta di servizio denominata April Patch Maintenance Window for App1 Prod for Account [account id]. Utilizza la richiesta del servizio patch per comunicare con AMS se hai bisogno di modifiche alla patch pianificata o per saltare una patch imminente. Quando viene creata una richiesta di assistenza, viene inviata un'e-mail all'indirizzo di notifica della patch con un link alla richiesta di servizio. Riceverai un'e-mail aggiuntiva ogni volta che AMS aggiorna la richiesta di servizio.

> **Note**
>
> AMS crea una nuova richiesta di servizio, anche se la finestra di manutenzione delle patch viene creata meno di quattro giorni prima della sua esecuzione programmata.
> La finestra di manutenzione delle patch deve essere in uno stato «abilitato» per ricevere le notifiche di richiesta di assistenza.

Un'ora prima dell'inizio dell'applicazione delle patch, AMS invia una notifica all'utente tramite la richiesta del servizio di patch. Al termine dell'applicazione delle patch, AMS aggiorna la richiesta del servizio di patch con un collegamento alla console Patch Manager. Utilizza il link per visualizzare la conformità delle patch per le istanze prese di mira dalla finestra di manutenzione delle patch.

> **Note**
>
> I collegamenti nella console Patch Manager mostrano la conformità attuale delle istanze. Patch Manager mostra un'istanza come non conforme se vengono rilasciate nuove patch tra il momento in cui AMS completa l'applicazione delle patch e l'accesso al collegamento.

CloudWatch Notifiche di patch tramite Events

AMS invia CloudWatch gli eventi tre volte durante il processo di patch, tra cui:

- Quattro giorni prima dell'avvio della finestra di manutenzione delle patch.
- Un'ora prima dell'esecuzione della finestra di manutenzione delle patch.
- Al termine della finestra di manutenzione delle patch.

Di seguito è riportato lo schema degli eventi di notifica avanzata di Patch Maintenance Window:

```
{
    "version": "0",
    "id": "37004d81-458d-2cef-fe1c-8afa8af30406",
    "detail-type": "AMS Patch Window Execution State Change",
    "source": "aws.managedservices",
    "account": "145917996532",
    "time": "2021-05-20T02:00:00Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ssm:us-east-1:123456789012:maintenancewindow/mw-00000001235",
        "arn:aws:ec2:us-east-1:123456789012:instance/i-0000000aaaaaaaaaa",
        "arn:aws:ec2:us-east-1:123456789012:instance/i-0000000aaaaaaaaab"
    ],
    "detail": {
        "State": "PREEMPTIVE",
        "StartTime": "2021-05-24T02:00:00.000000",
        "WindowArn": "arn:aws:ssm:us-east-1:123456789012:maintenancewindow/
mw-00000001235",
        "Results": "[{\"instanceId\": \"i-0000000aaaaaaaaaa\"}, {\"instanceId\":
 \"i-0000000aaaaaaaaab\"}]"
    }
}
```

La tabella seguente descrive lo schema degli eventi di notifica anticipata di Patch Maintenance Window:

Dettagli della notifica delle patch

Nome proprietà	Descrizione	Valori di esempio
Stato	Lo stato della finestra di manutenzione delle patch	PREEMPTIVE: la finestra di applicazione delle patch programmata per iniziare a breve
Stato	Lo stato della finestra di manutenzione dell'appl icazione delle patch	OPERAZIONE RIUSCITA: tutte le istanze sono state patchate senza errori

Nome proprietà	Descrizione	Valori di esempio
		FALLITO: non è stato possibile applicare la patch ad almeno un'istanza
StartTime	L'ora di inizio, in formato ISO, della finestra di manutenzione dell'applicazione delle patch	2021-02-03T 22:14:05.814 308
WindowArn	L'identificatore univoco della finestra di manutenzione delle patch	arn:aws:ssm:us-east-1:12345 6789012:maintenance window/mw-00000001235
Risultati	L'elenco delle istanze prese di mira dalla finestra di patch	InstanceId — l'ID dell'istanza di destinazione

Di seguito è riportato lo schema degli eventi di fine della finestra di manutenzione delle patch:

```
{"version": "0",
    "id": "0f25add5-44a9-0702-d2bc-bd2102affefe",
    "detail-type": "AMS Patch Window Execution State Change",
    "source": "aws.managedservices",
    "account": "123456789012",
    "time": "2021-02-03T22:14:06Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ssm:us-east-1:123456789012:maintenancewindow/mw-00000001235",
        "arn:aws:ec2:us-east-1:123456789012:instance/i-0000000aaaaaaaaaa",
        "arn:aws:ec2:us-east-1:123456789012:instance/i-0000000aaaaaaaaab"
    ],
    "detail": {"State": "[COMPLETED]",
        "Status": "SUCCESS",
        "StartTime": "2021-02-03T22:12:00.814308",
        "EndTime": "2021-02-03T22:14:05.814309",
        "WindowArn": "arn:aws:ssm:us-east-1:123456789012:maintenancewindow/
mw-00000001235",
        "WindowExecutionId": "e32088eb-c05f-4c63-b766-6866e163c818",
        "Results": "[{\"instanceId\": \"i-0000000aaaaaaaaaa\", \"status\":
 \"Success\", \"missing_critical_patch_count\": 0, \"missing_total_patch_count
```

```
\": 0} }, {\"instanceId\": \"i-0000000aaaaaaaaab\", \"status\": Success},
 \"missing_critical_patch_count\": 0, \"missing_total_patch_count\": 0}]"
    }
}
```

La tabella seguente descrive lo schema degli eventi di fine della finestra di manutenzione delle patch:

Dettagli di fine della finestra di patch

Nome proprietà	Descrizione	Valori di esempio
Stato	Lo stato della finestra di manutenzione delle patch	COMPLETATA: la finestra di applicazione delle patch è terminata
Stato	Lo stato della finestra di manutenzione dell'appl icazione delle patch	OPERAZIONE RIUSCITA: tutte le istanze sono state patchate senza errori FALLITO: non è stato possibile applicare la patch ad almeno un'istanza
StartTime	L'ora di inizio, in formato ISO, della finestra di manutenzione dell'applicazione delle patch	2021-02-03T 22:14:05.814 308
EndTime	L'ora di fine, in formato ISO, della finestra di manutenzione dell'applicazione delle patch	2021-02-03T 23:14:05.814 308
WindowArn	L'identificatore univoco della finestra di manutenzione delle patch.	arn:aws:ssm:us-east-1:12345 6789012:manutancewindow/ mw-00000001235
WindowExecutionId	L'ID di esecuzione della finestra, che può essere visualizzato dalla console SSM Maintenance Window	e32088eb-c05f-4c63- b766-6866e163c818

Nome proprietà	Descrizione	Valori di esempio
Risultati	L'elenco delle istanze che verranno prese di mira dalla finestra di patch	InstanceId — l'ID dell'istanza bersaglio status: lo stato della patch dell'istanza missing_critical_patch_count - il conteggio delle patch critiche mancanti sull'istanza missing_total_patch_count - il numero totale di patch mancanti sull'istanza

È possibile utilizzare l'evento CloudWatch Events per attivare una CloudWatch regola che avvisa l'utente quando viene inviato un avviso anticipato di Patching Maintenance Window. A tale scopo, configura la CloudWatch regola con la seguente configurazione:

```
{
    "source": [
        "aws.managedservices"
    ],
    "detail-type": [
        "AMS Patch Window Execution State Change"
    ],
    "detail": {
        "State": ["PREEMPTIVE"]
    }
}
```

> **Note**
>
> Gli avvisi di errore delle patch non vengono creati per le istanze con sistemi operativi non supportati o che vengono interrotte durante la finestra di manutenzione.

Indagine sugli errori delle patch in AMS

AWS Managed Services (AMS) gestisce l'applicazione delle patch e include la correzione degli errori delle patch. Quando l'applicazione delle patch fallisce, AMS Operations viene avvisata e tenta di risolvere il problema seguendo le AWS migliori pratiche di AMS per risolvere il problema.

<instance-id>Se una patch fallisce, AMS crea un SSM OpsItem nell'account con il seguente titolo: AWS Managed Services — Patch Instance failure per esempio.

AMS quindi esamina il. OpsItem Se AMS è in grado di correggere l'errore senza l'intervento dell'utente, allora AMS risolve il problema. OpsItem Se è necessario un intervento, AMS invia una notifica all'utente tramite una richiesta di assistenza contenente i risultati dell'indagine e le procedure di riparazione consigliate. Se non intraprendi alcuna azione per risolvere il problema, AMS tenta di applicare una patch all'istanza durante la successiva finestra di manutenzione programmata delle patch.

> **Note**
>
> OpsItems Gli errori di patch non vengono creati per le istanze con sistemi operativi non supportati o che si trovano nello stato Interrotto durante la finestra di manutenzione delle patch.

Ottimizzazione dei costi con AMS Resource Scheduler

La AWS soluzione AMS Resource Scheduler on ti aiuta a ridurre i costi tuoi AWS e di AMS bloccando le risorse non utilizzate e avviando le risorse quando è necessaria la capacità. Ad esempio, puoi utilizzare AMS Resource Scheduler on AWS in un ambiente di sviluppo per interrompere automaticamente le istanze al di fuori dell'orario lavorativo ogni giorno. Se lasci tutte le istanze in esecuzione al massimo, questa soluzione può ridurre l'utilizzo delle istanze, con conseguente riduzione dei costi complessivi in base alle pianificazioni configurate.

Usa AWS Managed Services (AMS) Resource Scheduler per pianificare l'avvio e l'arresto automatici dei gruppi di Auto Scaling, delle istanze EC2 Amazon e delle istanze Amazon RDS nel tuo account. Questo aiuta a ridurre i costi di infrastruttura laddove le risorse non sono destinate a funzionare 24 ore su 24, 7 giorni su 7. La soluzione si basa su AWS Instance Scheduler ma contiene funzionalità e personalizzazioni aggiuntive specifiche per le esigenze dei clienti AMS. La personalizzazione include il supporto per la pianificazione dei gruppi Auto Scaling CloudWatch , il soppressore degli allarmi per gli allarmi Elastic Load Balancing, il supporto per AWS Systems Manager più finestre di manutenzione per EC2 Amazon, uno strumento per la stima dei risparmi sui costi e il supporto operativo di AMS.

AMS Resource Scheduler utilizza periodi e pianificazioni. I periodi definiscono gli orari in cui la risorsa deve essere eseguita, ad esempio l'ora di inizio, l'ora di fine e i giorni del mese. Le pianificazioni contengono i periodi definiti, insieme a configurazioni aggiuntive (finestra di manutenzione SSM, fuso orario, ibernazione, ecc.) e specificano quando le risorse devono essere eseguite. Puoi configurare questi periodi e pianificazioni utilizzando i runbook di automazione forniti da AMS. AWS Systems Manager Ogni pianificazione deve contenere almeno un periodo che definisce l'ora o le ore in cui l'istanza deve essere eseguita. Una pianificazione può contenere più di un periodo. Quando in una pianificazione vengono utilizzati più periodi, Instance Scheduler applica l'azione di avvio appropriata quando almeno una delle regole del periodo è vera. Per ulteriori dettagli su pianificazione e periodi, consulta Solutions Components of AWS Instance Scheduler.

AMS Resource Scheduler utilizza i tag delle AWS risorse per associare una pianificazione a una o più risorse in modo da indirizzarle alle azioni di avvio e arresto pianificate. Etichetti le tue risorse con la chiave tag (quella predefinita`Schedule`) configurata nello Scheduler con il nome della pianificazione come valore. Si configura la stessa chiave di tag del tag di allocazione dei costi AWS Cost Explorer per la funzionalità di stima dei costi di Scheduler per tracciare e generare report sui risparmi sui costi.

AMS Resource Scheduler è una funzionalità opzionale che puoi abilitare per account.

Utilizzo delle risorse con AMS Resource Scheduler

Amazon EC2

- Le EC2 istanze Amazon che fanno parte di un gruppo Auto Scaling non vengono elaborate singolarmente e ignorate da AMS Resource Scheduler, anche se sono contrassegnate.
- Se il volume root dell'istanza di destinazione è crittografato con una chiave master AWS KMS del cliente (CMK), è necessario aggiungere un'`kms:CreateGrant`autorizzazione aggiuntiva al ruolo IAM di Resource Scheduler, affinché lo scheduler possa avviare tali istanze. Per impostazione predefinita, questa autorizzazione non viene aggiunta al ruolo per una maggiore sicurezza. Se richiedi questa autorizzazione, puoi aggiungere l'autorizzazione aggiornando lo CloudFormation stack`ams-resource-scheduler`, con un elenco di CMK come valore del `UseCMK` parametro (usa una o più chiavi CMK ARNs nel formato `arn:`*`partition`*`:kms:`*`region`*`:`*`account-id`*`:key/`*`key-id`* anziché un alias KMS).
- Se le tue EC2 istanze Amazon sono configurate con software specifico o licenze del fornitore gestite da AWS License Manager, Resource Scheduler necessita delle autorizzazioni per le AWS License Manager licenze specifiche per poter avviare l'istanza. È possibile concedere a Resource Scheduler le autorizzazioni necessarie aggiungendo l'elenco degli ARN delle licenze alla licenza del gestore delle AWS License Manager licenze, EC2 ad esempio il parametro dello stack (). CloudFormation `ams-resource-scheduler`

Amazon EC2 Auto Scaling

- AMS Resource Scheduler avvia o arresta la scalabilità automatica dei gruppi di Auto Scaling, non delle singole istanze del gruppo. Cioè, lo scheduler ripristina la dimensione del gruppo Auto Scaling (inizio) o imposta la dimensione su 0 (arresto).
- Etichetta il gruppo Auto Scaling con il tag specificato e non le istanze all'interno del gruppo.
- Durante l'arresto, AMS Resource Scheduler memorizza i valori di capacità minima, desiderata e massima del gruppo Auto Scaling e imposta la capacità minima e desiderata su 0. Durante l'avvio, lo scheduler ripristina la dimensione del gruppo Auto Scaling com'era durante l'arresto. Pertanto, le istanze del gruppo Auto Scaling devono utilizzare una configurazione di capacità appropriata in modo che la chiusura e il riavvio delle istanze non influiscano su alcuna applicazione in esecuzione nel gruppo Auto Scaling.
- Se il gruppo Auto Scaling viene modificato (la capacità minima o massima) durante un periodo di esecuzione, lo scheduler memorizza la nuova dimensione del gruppo Auto Scaling e la utilizza per ripristinare il gruppo al termine di una pianificazione di interruzioni.

Amazon RDS

- Lo scheduler può scattare un'istantanea prima di arrestare le istanze RDS (non si applica al cluster Aurora DB). Questa funzionalità è attivata per impostazione predefinita con il parametro del CloudFormation modello Create RDS Instance Snapshot AWS impostato su true. Lo snapshot viene conservato fino alla successiva interruzione dell'istanza Amazon RDS e alla creazione di una nuova istantanea.
- Scheduler può utilizzare istanze start/stop Amazon RDS che fanno parte di un cluster o di un database Amazon RDS Aurora o in una configurazione con più zone di disponibilità (Multi-AZ). Tuttavia, controlla la limitazione di Amazon RDS quando lo scheduler non sarà in grado di interrompere l'istanza Amazon RDS, in particolare le istanze Multi-AZ.
- Per pianificare l'avvio o l'arresto di Aurora Cluster, usa il parametro del modello Schedule Aurora Clusters (l'impostazione predefinita è true). Il cluster Aurora (non le singole istanze all'interno del cluster) deve essere etichettato con la chiave tag definita durante la configurazione iniziale e il nome della pianificazione come valore del tag per pianificare quel cluster.

> **Note**
>
> Il Resource Scheduler non verifica che una risorsa sia avviata o interrotta. Effettua la chiamata API per il servizio pertinente e prosegue. Se la chiamata API fallisce, registra l'errore per consentirne l'analisi.
> AMS Resource Scheduler non supporta AWS Backup Windows. Se si mappa un'istanza RDS AWS Backup abilitata con la pianificazione di Resource Scheduler, affinché il backup funzioni come previsto, la finestra di backup deve trovarsi all'interno della finestra di esecuzione della pianificazione.

Onboarding AMS Resource Scheduler

Il tuo account non viene automaticamente inserito in AMS Resource Scheduler quando viene inserito nel piano operativo AMS Accelerate. Tuttavia, come parte dell'onboarding dell'account nel piano operativo AMS Accelerate, o in qualsiasi momento successivo, puoi richiedere al Cloud Service Delivery Manager (CSDM) di effettuare l'onboarding dell'account su AMS Resource Scheduler. Una volta che il CSDM ha effettuato l'onboard dell'account, nel tuo account viene automaticamente fornito uno CloudFormation stack contenente le risorse AMS Resource Scheduler con configurazione predefinita.

Dopo aver effettuato il provisioning di AMS Resource Scheduler nel tuo account, ti consigliamo di rivedere la configurazione predefinita e, se necessario, personalizzare configurazioni come tag key, fuso orario, servizi pianificati e così via, in base alle tue preferenze. Per i dettagli sulle personalizzazioni consigliate, consulta la sezione successiva. Personalizzazione di AMS Resource Scheduler

Personalizzazione di AMS Resource Scheduler

Una volta effettuato l'onboarding, AMS Resource Scheduler viene distribuito come CloudFormation stack, con nome, `ams-resource-scheduler` nella regione AWS principale del tuo account AMS Accelerate. Puoi configurare le proprietà di AMS Resource Scheduler in base alle tue preferenze tramite i parametri dello stack ed eseguendo un aggiornamento CloudFormation dello stack. Per informazioni sull'aggiornamento degli CloudFormation stack, consulta Aggiornamento diretto degli stack.

Ti consigliamo di personalizzare le seguenti proprietà e lasciare il resto come predefinito per una funzionalità ottimale.

- Nome tag: il nome del tag che Resource Scheduler utilizzerà per associare le pianificazioni delle istanze alle risorse. Il valore predefinito è `Schedule`.
- Servizi da pianificare: un elenco separato da virgole di servizi che Resource Scheduler può gestire. Il valore predefinito è "`ec2,rds,autoscaling`". I valori validi sono «ec2", «rds» e «autoscaling».
- Fuso orario predefinito: specifica il fuso orario predefinito da utilizzare per il Resource Scheduler. Il valore predefinito è `UTC`.
- CMK per volumi EBS crittografati: un elenco separato da virgole di Amazon KMS Customer Managed Key (CMK ARNs) a cui è possibile concedere le autorizzazioni a Resource Scheduler.
- Licenza di gestione delle licenze, EC2 ad esempio: è possibile concedere autorizzazioni a un elenco separato da virgole di AWS Licence Manager ARNs a quel Resource Scheduler.

> **Note**
>
> AMS rilascia occasionalmente funzionalità e correzioni per mantenere aggiornato AMS Resource Scheduler nel tuo account. Quando ciò accade, tutte le personalizzazioni apportate allo stack AMS Resource Scheduler tramite i parametri dello stack vengono mantenute.

Sconsigliamo vivamente di effettuare personalizzazioni dirette a qualsiasi risorsa componente di AMS Resource Scheduler. Ciò influisce sulla funzionalità di Resource Scheduler e sulla capacità di AMS di mantenerlo aggiornato.

Utilizzo di AMS Resource Scheduler

Come utilizzare i periodi AMS Resource Scheduler negli account AMS Accelerate.

Utilizza il seguente set di runbook di AWS Systems Manager automazione per amministrare la pianificazione e il periodo richiesti in AMS Resource Scheduler.

Note

Questi runbook di automazione SSM sono disponibili nella regione AWS principale del tuo account.

- `AWSManagedServices-AddOrUpdatePeriod`
- `AWSManagedServices-AddOrUpdateSchedule`
- `AWSManagedServices-DeleteScheduleOrPeriod`
- `AWSManagedServices-DescribeScheduleOrPeriods`
- `AWSManagedServices-EnableOrDisableAMSResourceScheduler`

Inoltre, AMS fornisce un AWS Identity and Access Management ruolo che AWS Systems Manager richiede e assume per poter utilizzare i runbook. `ams_resource_scheduler_ssm_automation_role` Il ruolo IAM è limitato a una politica in linea con privilegi minimi che concede le autorizzazioni SSM necessarie per la funzionalità dei runbook.

Prerequisiti

Esegui i seguenti passaggi prima di iniziare a utilizzare il runbook di automazione SSM e AMS Resource Scheduler.

Allega la seguente policy all'entità IAM appropriata (utente, gruppo o ruolo) a cui desideri consentire l'utilizzo dei runbook di automazione per amministrare la pianificazione e il periodo in AMS Resource Scheduler. La policy non è richiesta se l'entità IAM dispone dell'autorizzazione di amministratore o dell' PowerUser autorizzazione nel proprio account.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowPassingResourceSchedulerRole",
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::111122223333:role/
ams_resource_scheduler_ssm_automation_role",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "ssm.amazonaws.com"
                }
            }
        },
        {
            "Sid": "ListAndDescribeAutomationExecutions",
            "Effect": "Allow",
            "Action": [
                "ssm:GetAutomationExecution",
                "ssm:DescribeAutomationStepExecutions"
            ],
            "Resource": "arn:aws:ssm:*:111122223333:automation-execution/*"
        },
        {
            "Sid": "ListAndDescribeResourceSchedulerSSMDocuments",
            "Effect": "Allow",
            "Action": [
                "ssm:ListDocumentVersions",
                "ssm:DescribeDocument",
                "ssm:ListDocumentMetadataHistory",
                "ssm:DescribeDocumentParameters",
                "ssm:GetDocument",
                "ssm:DescribeDocumentPermission"
            ],
            "Resource": [
                "arn:aws:ssm:*::document/AWSManagedServices-AddOrUpdatePeriod",
                "arn:aws:ssm:*::document/AWSManagedServices-AddOrUpdateSchedule",
                "arn:aws:ssm:*::document/AWSManagedServices-
DeleteScheduleOrPeriod",
```

```
                "arn:aws:ssm:*::document/AWSManagedServices-
DescribeScheduleOrPeriods",
                "arn:aws:ssm:*::document/AWSManagedServices-
EnableOrDisableAMSResourceScheduler"
            ]
        },
        {
            "Sid": "AllowExecutionOfResourceSchedulerSSMDocuments",
            "Effect": "Allow",
            "Action": [
                "ssm:StartAutomationExecution"
            ],
            "Resource": [
                "arn:aws:ssm:*::document/AWSManagedServices-AddOrUpdatePeriod",
                "arn:aws:ssm:*::document/AWSManagedServices-AddOrUpdateSchedule",
                "arn:aws:ssm:*::document/AWSManagedServices-
DeleteScheduleOrPeriod",
                "arn:aws:ssm:*::document/AWSManagedServices-
DescribeScheduleOrPeriods",
                "arn:aws:ssm:*::document/AWSManagedServices-
EnableOrDisableAMSResourceScheduler",
                "arn:aws:ssm:*:111122223333:automation-execution/*"
            ]
        },
        {
            "Sid": "AllowListingAllDocuments",
            "Effect": "Allow",
            "Action": "ssm:ListDocuments",
            "Resource": "*"
        },
        {
            "Sid": "AllowListingAllSSMExecutions",
            "Effect": "Allow",
            "Action": "ssm:DescribeAutomationExecutions",
            "Resource": "*"
        },
        {
            "Sid": "AllowListingIAMRolesForStartingExecutionViaConsole",
            "Effect": "Allow",
            "Action": "iam:ListRoles",
            "Resource": "*"
        }
    ]
```

```
}
```

È possibile eseguire l'automazione dalla AWS Systems Manager console o utilizzando la AWS CLI. Se si utilizza la AWS CLI, potrebbe essere necessario installarla e configurarla o gli AWS strumenti per PowerShell, se non l'hai già fatto. Per informazioni, consulta Installare o aggiornare gli strumenti da AWS riga di comando.

Guarda il video di Navish per saperne di più (4:52)

Utilizzo di periodi e pianificazioni in AWS Managed Services Resource Scheduler

Puoi utilizzare AMS Resource Scheduler per aggiungere, aggiornare o eliminare pianificazioni o periodi negli account AMS Accelerate.

Aggiungere o aggiornare periodi in AMS Resource Scheduler

Aggiungi o aggiorna un periodo di Resource Scheduler nei tuoi account AMS.

Dati di cui avrai bisogno:

- Azione: il tipo di operazione da eseguire. Usa «aggiungi» se desideri aggiungere un periodo o «aggiorna» se desideri aggiornare un periodo esistente.
- Nome: il nome del periodo. È necessario specificare un valore univoco se si aggiunge un nuovo periodo.
- AutomationAssumeRole: L'ARN del ruolo AWS Identity and Access Management (IAM) che consente al runbook di aggiungere o aggiornare il periodo per tuo conto. Specificate il ruolo come. `ams_resource_scheduler_ssm_automation_role`
- Descrizione (facoltativa): una descrizione significativa del periodo.
- BeginTime(Facoltativo): L'ora in formato HH:MM in cui desideri avviare le risorse.
- EndTime(Facoltativo): L'ora in formato HH:MM in cui desideri interrompere le risorse.
- Mesi (facoltativo): un elenco di mesi delimitato da virgole o un intervallo di mesi sillabato durante i quali le risorse devono essere eseguite.
- MonthDays(Facoltativo): un elenco di giorni del mese delimitato da virgole o un intervallo di giorni con sillabazione durante i quali le risorse devono essere eseguite.
- WeekDays(Facoltativo): un elenco delimitato da virgole dei giorni della settimana o di un intervallo di giorni della settimana in cui devono funzionare le risorse.

Come farlo:

- Visualizza il documento all'indirizzo AWSManagedServices-AddOrUpdatePeriod(potrebbe essere necessario scegliere la regione di imbarco).

  Specificate i requisiti nella sezione Parametri di input, quindi scegliete Esegui. Al termine dell'operazione, visualizza i risultati nella scheda Output.

- AWS CLI:

  Esegui il comando seguente per avviare un'automazione. Sostituiscilo *placeholders* con le tue informazioni.

```
aws ssm start-automation-execution --document-name "AWSManagedServices-
AddOrUpdatePeriod" --document-version "\$DEFAULT"
     --parameters '{"Action":["add" or "update"], "Name":["NAME"],
    "Description":["DESCRIPTION"],"BeginTime":["TIME"], "EndTime":["TIME"],
    "Months":["MONTH"],"MonthDays":["DAY"], "WeekDays":["DAY"],
    "AutomationAssumeRole" : ["arn:aws:iam::ACCOUNTID:role/
ams_resource_scheduler_ssm_automation_role"] }' --region ONBOARDED_REGION
```

Esempio:

L'esempio seguente mostra come aggiungere un nuovo periodo utilizzando la AWS Systems Manager console. Abbiamo denominato il periodo Period-Name e lo abbiamo configurato in modo che copra le 9:00-18:00 dal lunedì al venerdì per i primi 15 giorni di ogni mese.

1. Visualizza il documento di AWS Systems Manager automazione all'indirizzo AWSManagedServices-AddOrUpdatePeriod(potresti dover scegliere la regione di registrazione).

2. Fornisci i valori per i parametri.

3. Fai clic su Esegui e attendi il completamento dell'automazione.

Aggiungere o aggiornare le pianificazioni in AMS Resource Scheduler

Aggiungi o aggiorna una pianificazione di Resource Scheduler negli account AMS Accelerate.

Dati di cui avrai bisogno:

- Azione: il tipo di operazione da eseguire. Usa «aggiungi» se desideri aggiungere una pianificazione o «aggiorna» se desideri aggiornare una pianificazione esistente.
- Nome: il nome della pianificazione. È necessario specificare un valore univoco se si aggiunge una nuova pianificazione.
- AutomationAssumeRole: L'ARN del ruolo AWS Identity and Access Management (IAM) che consente al runbook di aggiungere o aggiornare la pianificazione per tuo conto. Specificate il ruolo. `ams_resource_scheduler_ssm_automation_role`
- Descrizione (facoltativa): una descrizione significativa della pianificazione.
- Periodi (facoltativo): specifica un elenco delimitato da virgole di periodi da utilizzare con questa pianificazione. Ogni periodo deve essere già stato creato.
- RetainRunning(Facoltativo): Specificate «true» per evitare che Resource Scheduler interrompa una risorsa in esecuzione alla fine di un periodo di esecuzione se la risorsa è stata avviata manualmente prima dell'inizio del periodo di esecuzione. Per impostazione predefinita, Resource Scheduler arresta la risorsa.
- StopNewInstances(Facoltativo): Specificate «false» per evitare che Resource Scheduler interrompa una risorsa la prima volta che viene etichettata se è in esecuzione al di fuori del periodo di esecuzione. Per impostazione predefinita, Resource Scheduler arresta la risorsa.
- SSMMaintenanceFinestra (opzionale): specifica un elenco delimitato da virgole di finestre di manutenzione di AWS Systems Manager (SSM) che desideri aggiungere come periodi di esecuzione per la pianificazione. È inoltre necessario specificare la proprietà "UseMaintenanceWindow" su «true».
- TimeZone(Facoltativo): Specificate il fuso orario che desiderate che Resource Scheduler utilizzi. Per impostazione predefinita, Resource Scheduler utilizza l'UTC.
- UseMaintenanceWindow(Facoltativo): specifica «true» se desideri che Resource Scheduler consideri la finestra di manutenzione di Amazon Relational Database Service (RDS) come periodo di esecuzione per la pianificazione di un'istanza Amazon RDS o per aggiungere finestre di manutenzione di AWS Systems Manager (SSM) come periodo di esecuzione alla pianificazione di un'istanza Amazon EC2.
- UseMetrics(Facoltativo): specifica «true» per abilitare le CloudWatch metriche a livello di pianificazione e «false» per disabilitarle. CloudWatch La specificazione di questa proprietà ha la precedenza sull'impostazione delle CloudWatch metriche impostata a livello di stack.

Come farlo:

- Visualizza il documento all'indirizzo AWSManagedServices-AddOrUpdateSchedule(potrebbe essere necessario scegliere la regione di imbarco).

  Specificate i requisiti nella sezione Parametri di input, quindi scegliete Esegui. Al termine dell'operazione, visualizza i risultati nella scheda Output.

- AWS CLI:

  Esegui il comando seguente per avviare un'automazione. Sostituiscilo *placeholders* con le tue informazioni.

```
aws ssm start-automation-execution --document-name "AWSManagedServices-
AddOrUpdateSchedule" --document-version "\$DEFAULT"
     --parameters '{"Action":["add" or "update"], "Name":["NAME"], "Description":
["DESCRIPTION"],
    "Hibernate":["true or false"],"Enforced":["true or false"],
    "OverrideStatus":["running or stopped"],"Periods":["PERIOD-A, PERIOD-B"],
    "RetainRunning":["true or false"],"StopNewInstances":["true or false"],
    "SSMMaintenanceWindow":["WINDOW-NAME"],"TimeZone":["TIMEZONE"],
    "UseMaintenanceWindow":["true or false"],"UseMetrics":["true or false"],
    "AutomationAssumeRole" : ["arn:aws:iam::ACCOUNTID:role/
ams_resource_scheduler_ssm_automation_role"] }' --region ONBOARDED_REGION
```

Esempio:

L'esempio seguente mostra come aggiungere una pianificazione per AMS Resource Scheduler. In questo esempio si aggiunge una pianificazione denominata using. CustomSchedule CustomPeriod

1. Visualizza il documento di AWS Systems Manager automazione all'indirizzo AWSManagedServices-AddOrUpdateSchedule(potrebbe essere necessario scegliere la regione di registrazione).

2. Fornisci i valori per i parametri.

3. Fai clic su Esegui e attendi il completamento dell'automazione.

Eliminazione di periodi o pianificazioni in AMS Resource Scheduler

Per eliminare i periodi o le pianificazioni di Resource Scheduler negli account AMS Accelerate, sono necessari i seguenti dati:

- ConfigurationType: Il tipo di configurazione che desideri eliminare. Usa «periodo» se desideri eliminare i periodi o «pianificazione» se desideri eliminare le pianificazioni.
- Nome: il nome della pianificazione o del periodo che desideri eliminare.
- AutomationAssumeRole: L'ARN del ruolo AWS Identity and Access Management (IAM) che consente al runbook di eliminare pianificazioni o periodi per tuo conto. Specificare il ruolo. `ams_resource_scheduler_ssm_automation_role`

Come farlo:

- Visualizza il documento all'indirizzo AWSManagedServices-DeleteScheduleOrPeriod(potresti dover scegliere la regione di registrazione).

  Specificate i requisiti nella sezione Parametri di input, quindi scegliete Esegui. Al termine dell'operazione, visualizza i risultati nella scheda Output.
- AWS CLI:

  Esegui il comando seguente per avviare un'automazione. Sostituiscilo *`placeholders`* con le tue informazioni.

```
aws ssm start-automation-execution --document-name "AWSManagedServices-
DeleteScheduleOrPeriod" --document-version "\$DEFAULT"
--parameters '{"ConfigurationType":["period" or "schedule"],"Name":["NAME"],
    "AutomationAssumeRole":["arn:aws:iam::ACCOUNTID:role/
ams_resource_scheduler_ssm_automation_role"]}' --region ONBOARDED_REGION
```

Esempio:

L'esempio seguente mostra come eliminare un periodo utilizzando la AWS Systems Manager console.

1. Visualizza il documento di AWS Systems Manager automazione all'indirizzo AWSManagedServices-DeleteScheduleOrPeriod(potrebbe essere necessario scegliere la regione di registrazione).

2. Fornisci i valori per i parametri.

3. Fai clic su Esegui e attendi il completamento dell'automazione.

Descrizione di periodi o pianificazioni in AMS Resource Scheduler

Per descrivere (visualizzare i dettagli) un periodo o una pianificazione di Resource Scheduler negli account AMS Accelerate, sono necessari i seguenti dati:

- ConfigurationType: Il tipo di configurazione che vuoi descrivere. Usa «periodi» se vuoi descrivere tutti i periodi o «orari» se vuoi descrivere tutti gli orari.
- AutomationAssumeRole: L'ARN del ruolo AWS Identity and Access Management (IAM) che consente al runbook di descrivere pianificazioni o periodi per tuo conto. Specificare il ruolo. `ams_resource_scheduler_ssm_automation_role`

Come farlo:

- Visualizza il documento all'indirizzo AWSManagedServices-DescribeScheduleOrPeriods(potrebbe essere necessario scegliere la regione di registrazione):
  1. Specificate i requisiti nella sezione Parametri di input, quindi scegliete Esegui.
  2. Al termine dell'operazione, visualizza i risultati nella scheda Output.
- AWS CLI:
  1. Esegui il comando seguente per avviare un'automazione. Sostituiscilo *`placeholders`* con le tue informazioni.

```
aws ssm start-automation-execution --document-name "AWSManagedServices-
DescribeScheduleOrPeriods" --document-version "\$DEFAULT"
                --parameters '{"ConfigurationType":["period" or
 "schedule"],"AutomationAssumeRole":["arn:aws:iam::ACCOUNTID:role/
ams_resource_scheduler_ssm_automation_role"]}'
                --region ONBOARDED_REGION
```

Esempio:

L'esempio seguente mostra come descrivere un periodo utilizzando la AWS Systems Manager console.

1. Visualizza il documento di AWS Systems Manager automazione all'indirizzo AWSManagedServices-DescribeScheduleOrPeriods(potrebbe essere necessario scegliere la regione di registrazione).

2. Fornisci i valori per i parametri.

3. Fai clic su Esegui e attendi il completamento dell'automazione.

Taggare le risorse per AMS Resource Scheduler

Risorse di etichettatura per AMS Resource Scheduler.

Dopo aver aggiunto pianificazioni e periodi ad AMS Resource Schedule, devi etichettare le tue risorse con il nome del tag Resource Scheduler come chiave del tag, o quello personalizzato, e il nome della pianificazione come valore del tag. Per i dettagli su come etichettare le risorse nel tuo account AMS Accelerate, consultaEtichettatura in AMS Accelerate.

> **Note**
>
> Se si utilizza Resource Tagger per etichettare le risorse, la chiave Tag predefinita per Resource Scheduler deve essere personalizzata in modo da avere il prefisso '`ams:rt:`' poiché tutti i tag applicati dal resource tagger hanno il prefisso chiave ". `ams:rt:` In caso contrario, le risorse contrassegnate con resource tagger non saranno gestite da Resource Scheduler. Per ulteriori informazioni sulla personalizzazione della chiave Tag predefinita per Resource Scheduler, consulta. Personalizzazione di AMS Resource Scheduler

Stima dei costi in AMS Resource Scheduler

Per tenere traccia dei risparmi sui costi, AMS Resource Scheduler include un componente che calcola ogni ora i risparmi sui costi stimati per le risorse EC2 Amazon e Amazon RDS gestite dallo scheduler. Questi dati sui risparmi sui costi vengono quindi pubblicati come CloudWatch metrica (`AMS/ResourceScheduler`) per aiutarti a tenerne traccia. Lo strumento di stima dei costi stima i

risparmi solo sulle ore di funzionamento delle istanze. Non tiene conto di altri costi, come i costi di trasferimento dei dati associati a una risorsa.

Lo strumento di stima del risparmio sui costi è abilitato con Resource Scheduler. Funziona ogni ora e recupera i dati su costi e utilizzo da. AWS Cost Explorer Da questi dati calcola il costo orario medio per ogni tipo di istanza e quindi proietta il costo per un'intera giornata se l'istanza era in esecuzione senza pianificazione. Il risparmio sui costi è la differenza tra il costo previsto e il costo effettivo riportato da Cost Explorer per un determinato giorno.

Ad esempio, se l'istanza A è configurata con Resource Scheduler per essere eseguita dalle 9:00 alle 17:00, ovvero otto ore in un determinato giorno. Cost Explorer riporta il costo pari a $1 e l'utilizzo a 8. Il costo orario medio è quindi di 0,125 USD. Se l'istanza non è stata pianificata con Resource Scheduler, l'istanza verrà eseguita 24 ore su 24 in quel giorno. In tal caso, il costo sarebbe stato 24x0,125 = 3 USD. Resource Scheduler ti ha aiutato a ottenere un risparmio sui costi di 2$.

Affinché lo strumento di stima del risparmio dei costi recuperi i costi e l'utilizzo solo per le risorse gestite da Resource Scheduler da Cost Explorer, la chiave tag utilizzata da Resource Scheduler per indirizzare le risorse deve essere attivata come tag di allocazione dei costi nella dashboard di fatturazione. Se l'account appartiene a un'organizzazione, la chiave del tag deve essere attivata nell'account di gestione dell'organizzazione. Per informazioni su questa operazione, vedere Attivazione dei tag di allocazione dei costi definiti dall'utente e dei tag di allocazione dei costi definiti dall'utente

Dopo che la chiave tag è stata attivata come tag di allocazione dei costi, AWS billing inizia a tracciare i costi e l'utilizzo delle risorse gestite da Resource Scheduler e, una volta che i dati sono disponibili, lo strumento di stima dei costi inizia a calcolare i risparmi sui costi e a pubblicare i dati nello spazio dei nomi delle `AMS/ResourceScheduler` metriche in. CloudWatch

Se il tag di allocazione dei costi non è attivato, lo stimatore non è in grado di calcolare i risparmi e pubblicare la metrica, anche se è abilitata.

> **Note**
>
> Nel calcolo di Cost Savings Estimator non vengono presi in considerazione sconti come istanze riservate, piani di risparmio e così via. L'Estimator prende i costi di utilizzo da Cost Explorer e calcola il costo medio orario per le risorse. Per maggiori dettagli, consulta Understanding your AWS Cost Datasets: A Cheat Sheet.

Soppressore di allarmi in AMS Resource Scheduler

AMS Resource Scheduler è dotato di un CloudWatch dispositivo di soppressione degli allarmi, che viene distribuito come funzione Lambda separata denominata `AMSAlarmSuppressor` che sopprime gli allarmi per le istanze che sono alla base di Elastic Load Balancing, Application Load Balancer o Network Load Balancer. La funzione viene eseguita ogni 5 minuti, recupera tutti gli allarmi presenti nell'account e li raggruppa in base allo spazio dei nomi; ad esempio,,. `AWS/ELB` `AWS/ApplicationELB` `AWS/NetworkELB` Per ogni gruppo di allarmi, il soppressore trova il nome del load balancer, il gruppo target (per il gruppo and/or target) e controlla lo stato dell'istanza per ALB/NLB) from alarm dimensions, finds the instances that are registered with the load balancer and/or scoprire se le istanze sono pianificate da AMS Resource Scheduler. Se le istanze sono pianificate da Resource Scheduler e vengono interrotte da Resource Scheduler, il soppressore contrassegna quindi gli allarmi per disabilitarli. Se almeno un'istanza nell'elenco delle istanze registrate è in esecuzione, il dispositivo di soppressione contrassegna gli allarmi corrispondenti per abilitare gli allarmi contrassegnati per l'attivazione e disabilita gli allarmi contrassegnati per la disabilitazione. I log relativi a ciò vengono memorizzati nel gruppo di log. `/aws/lambda/AMSAlarmSuppressor`

Gestione dei log in AMS Accelerate

AMS Accelerate configura i AWS servizi supportati per raccogliere i log. Questi registri vengono utilizzati da AMS Accelerate per garantire la conformità e il controllo delle risorse all'interno dell'account.

AMS Accelerate offre una gamma di servizi operativi per aiutarti a raggiungere l'eccellenza operativa su AWS. Per comprendere rapidamente come AMS aiuta i tuoi team a raggiungere l'eccellenza operativa complessiva nel cloud AWS con alcune delle nostre funzionalità operative chiave, tra cui helpdesk 24 ore su 24, 7 giorni su 7, monitoraggio proattivo, sicurezza, patching, registrazione e backup, consulta i diagrammi dell'architettura di riferimento di AMS.

Argomenti

- Gestione dei log — AWS CloudTrail
- Gestione dei log — Amazon EC2
- Gestione dei log — Amazon VPC Flow Logs

Gestione dei log — AWS CloudTrail

AWS CloudTrailè un servizio utilizzato per la governance degli account: conformità, controllo operativo e controllo dei rischi. Con CloudTrail, puoi registrare, monitorare continuamente e conservare le attività dell'account relative alle azioni sull'infrastruttura AWS .

AMS Accelerate richiede AWS CloudTrail la registrazione per gestire gli audit e la conformità per tutte le risorse del tuo account. Durante l'onboarding, puoi scegliere una delle seguenti opzioni:

- Percorso distribuito da AMS: se scegli questa opzione, AMS crea, distribuisce e gestisce un percorso CloudTrail multiregionale nella tua AWS regione principale, indipendentemente dai percorsi esistenti nel tuo account.
- Porta il tuo percorso personale: se scegli di fornire il CloudTrail percorso del tuo account o della tua organizzazione, devi collaborare con Cloud Architect (CA) per assicurarti che soddisfi le configurazioni richieste per Accelerate. Se scegli questa opzione ma non fornisci il tuo percorso, Accelerate implementa automaticamente il proprio CloudTrail percorso per mantenere una copertura continua di sicurezza e audit. Se in un secondo momento fornisci la tua traccia personale, AMS rimuove la traccia utilizzata per evitare ridondanze e costi aggiuntivi. Questo

approccio aiuta a mantenere un unico CloudTrail percorso attivo nell'account ed evita la duplicazione dei costi di registrazione.

> **Note**
>
> Se il tuo account dispone di un CloudTrail percorso esistente e non hai specificamente configurato o richiesto un percorso gestito da AMS durante l'onboarding, AMS Accelerate rimuove automaticamente il percorso distribuito da AMS dal tuo account. In questo modo si evitano registrazioni duplicate, si ottimizza l'utilizzo delle risorse e si risparmiano costi aggiuntivi.

AMS Accelerate crea un bucket Amazon S3 per un CloudTrail percorso distribuito da Accelerate come destinazione di distribuzione degli eventi e utilizza AWS Key Management Service la crittografia ().AWS KMS Gli operatori di AMS Accelerate accedono ai tuoi eventi trail per scopi di indagine e diagnosi. Se sull'account è già abilitato un CloudTrail trail esistente, questo percorso si aggiunge a quello, se hai scelto di fare in modo che Accelerate implementasse un percorso gestito da Accelerate durante l'onboarding.

AMS Accelerate implementa AWS Config regole per garantire che i percorsi dei tuoi CloudTrail account, incluso un Accelerate deployed CloudTrail trail, siano configurati e crittografati correttamente. Per ulteriori informazioni, consulta AWS Config. Queste sono le regole utilizzate, presentate come collegamenti alla AWS documentazione che le descrive:

- multi-region-cloudtrail-enabled. Verifica che AMS Accelerate CloudTrail sia configurato correttamente con le configurazioni corrette.
- cloud-trail-encryption-enabled. Verifica che AWS CloudTrail sia configurato per utilizzare la crittografia lato server (SSE) con la crittografia della chiave master AWS KMS del cliente (CMK).
- cloud-trail-log-file-abilitato alla convalida. Se abilitato, verifica che AWS CloudTrail crei un file digest firmato con registri. Ti consigliamo vivamente di abilitare la convalida dei file su tutti i percorsi.
- s-3. bucket-default-lock-enabled Se abilitato, verifica che il bucket Amazon S3 abbia il blocco abilitato.
- s3 -. bucket-logging-enabled Se abilitato, verifica se la registrazione è abilitata per i bucket Amazon S3.

AMS Accelerate lo utilizza AWS KMS per crittografare gli eventi registrati per un percorso distribuito da CloudTrail Accelerate nel tuo account. Questa chiave è controllata ed è accessibile dagli amministratori degli account, dagli operatori di AMS Accelerate e. CloudTrail Per ulteriori informazioni AWS KMS, consulta la documentazione relativa AWS Key Management Service alle caratteristiche del prodotto.

Accesso e controllo dei log CloudTrail

CloudTrail i log per un CloudTrail percorso distribuito da AMS Accelerate sono archiviati in un bucket Amazon S3 all'interno del tuo account. I dati di trail archiviati nel bucket Amazon S3 sono crittografati utilizzando una chiave AWS KMS creata al momento del provisioning delle risorse. CloudTrail

I bucket Amazon S3 sfruttano un modello di denominazione ams-a ***aws account id***-cloudtrail-***AWS Region***, (esempio: ams-a123456789- -1a) e tutti gli eventi sono archiviati con il prefisso AWS/. cloudtrail-us-east CloudTrail Tutti gli accessi al bucket primario vengono registrati e gli oggetti di registro vengono crittografati e versionati per scopi di controllo.

Per ulteriori informazioni sulla registrazione delle modifiche e sull'interrogazione dei log, consulta. Monitoraggio delle modifiche nei tuoi account AMS Accelerate

Protezione e conservazione dei registri CloudTrail

AMS Accelerate consente il blocco degli oggetti di Amazon S3 con la modalità Governance per un CloudTrail percorso distribuito da Accelerate per garantire che gli utenti non possano sovrascrivere o eliminare una versione dell'oggetto o modificarne le impostazioni di blocco senza autorizzazioni speciali. Per ulteriori informazioni, consulta Amazon S3 object locking.

Per impostazione predefinita, tutti i log in questo bucket vengono conservati a tempo indeterminato. Se desideri modificare il periodo di conservazione, puoi inviare una richiesta di servizio tramite il Supporto AWS Centro per impostare una politica di conservazione diversa.

Accesso ai log di Amazon EC2

Puoi accedere ai log delle istanze di Amazon EC2 utilizzando. Console di gestione AWS I log prodotti da istanze e AWS servizi sono disponibili in CloudWatch Logs, disponibile in ogni account gestito da AMS Accelerate. Per informazioni sull'accesso ai log, consulta la documentazione dei log. CloudWatch

Conservazione dei log di Amazon EC2

Per impostazione predefinita, i log delle istanze di Amazon EC2 vengono conservati a tempo indeterminato. Se desideri modificare il periodo di conservazione, puoi inviare una richiesta di servizio tramite il Supporto AWS Centro per impostare una politica di conservazione diversa.

Gestione dei log — Amazon EC2

AMS Accelerate installa l' CloudWatch agente su tutte le istanze Amazon EC2 che hai identificato come gestite da AMS Accelerate. Questo agente invia log a livello di sistema ad Amazon Logs. CloudWatch Per informazioni, consulta Cosa sono Amazon CloudWatch Logs?

I seguenti file di log vengono inviati a CloudWatch Logs, in un gruppo di log con lo stesso nome del log. All'interno di ogni gruppo di log, viene creato un flusso di log per ogni istanza Amazon EC2, denominato in base all'ID dell'istanza Amazon EC2.

Linux

- /-ssm-agent.log var/log/amazon/ssm/amazon
- /var/log/amazon/ssm/errors.log
- /.log var/log/audit/audit
- /.log var/log/auth
- /-init-output.log var/log/cloud
- /var/log/cron
- /var/log/dnf.log
- /.log var/log/dpkg
- /var/log/maillog
- /var/log/messages
- /var/log/secure
- /var/log/spooler
- /var/log/syslog
- /.log var/log/yum
- /.log var/log/zypper

Per ulteriori informazioni, vedere Creare o modificare manualmente il file di configurazione CloudWatch dell'agente.

Windows

- SSMAgentRegistro Amazon
- AmazonCloudWatchAgentLog
- SSMErrorRegistro Amazon
- AmazonCloudFormationLog
- ApplicationEventLog
- EC2ConfigServiceEventLog
- MicrosoftWindowsAppLockerEXEAndDLLEventRegistro
- MicrosoftWindowsAppLockerMSIAndScriptEventLog
- MicrosoftWindowsGroupPolicyOperationalEventLog
- SecurityEventLog
- SystemEventLog

Per ulteriori informazioni, consulta Quick Start: abilitare le istanze Amazon EC2 che eseguono Windows Server 2016 per inviare log a log utilizzando Logs CloudWatch Agent. CloudWatch

Gestione dei log — Amazon VPC Flow Logs

VPC Flow Logs è una funzionalità che acquisisce informazioni sul traffico IP in entrata e in uscita dalle interfacce di rete del tuo VPC. I dati dei log di flusso possono essere pubblicati su Amazon CloudWatch logs o Amazon S3. La raccolta dei dati dei log di flusso non influisce sulla velocità effettiva o sulla latenza della rete. È possibile creare o eliminare i log di flusso senza alcun impatto sulle prestazioni della rete.

I log di flusso possono essere utili per diverse attività, ad esempio:

- Diagnosi delle regole eccessivamente restrittive del gruppo di sicurezza
- Monitoraggio del traffico che raggiunge l'istanza
- Identificazione della direzione del traffico da e verso le interfacce di rete

Non è necessario abilitare i log di flusso VPC per ogni VPC appena creato negli account Accelerate. AMS rileverà automaticamente se un VPC ha un log di flusso utilizzando la regola - ams-nist-cis-vpcConfig. flow-logs-enabled Se i log di flusso VPC non sono abilitati, AMS correggerà automaticamente il problema creando un log di flusso VPC con campi personalizzati. La disponibilità di questi campi aggiuntivi consentirà ad AMS e ai clienti di monitorare meglio il traffico VPC, comprendere le dipendenze della rete, risolvere i problemi di connettività di rete e identificare le minacce di rete.

Per informazioni sulla visualizzazione e la ricerca dei log di flusso, consulta Lavorare con i log di flusso.

Monitoraggio delle modifiche nei tuoi account AMS Accelerate

Important

Il servizio Change Record è obsoleto a partire dal 1° luglio 2025.
I nuovi account non possono essere inseriti nel servizio Change Record.
Per interrogare CloudTrail i dati nei tuoi account AMS Accelerate, puoi utilizzare questi servizi:

- In AWS CloudTrail, scegli Cronologia eventi e filtra gli eventi utilizzando gli attributi di ricerca. Puoi utilizzare il filtro dell'intervallo di tempo e scegliere di filtrare la cronologia degli eventi per origine degli eventi, come `s3.amazon.aws.com` specificato, oppure scegliere di filtrare la cronologia degli eventi per nome utente. Per ulteriori informazioni, consulta Lavorare con la cronologia CloudTrail degli eventi.
- Usa AWS CloudTrail Lake per raccogliere dati tramite query. In AWS CloudTrail scegli Lake, quindi scegli Query. Puoi creare query personalizzate, utilizzare il generatore di query o utilizzare query di esempio per raccogliere dati basati sugli eventi. Ad esempio, puoi chiedere chi ha eliminato un' EC2 istanza Amazon la settimana scorsa. Per ulteriori informazioni, consulta Creazione di un data lake da una AWS CloudTrail fonte e CloudTrailLake interrogazioni.
- Crea una tabella Amazon Athena AWS CloudTrail e imposta la posizione di archiviazione come bucket Amazon S3 associato al tuo percorso. Verifica che la regione iniziale del percorso e del bucket Amazon S3 coincidano. In Amazon Athena, usa l'editor di query per eseguire le query predefinite che Accelerate fornisce per l'uso con la console Athena. Per ulteriori informazioni su come creare una tabella Athena per interrogare i log, vedere Query CloudTrail logs. AWS CloudTrail

Argomenti

- Visualizzazione dei record delle modifiche
- Interrogazioni predefinite
- Modificare le autorizzazioni di registrazione

AWS Managed Services ti aiuta a tenere traccia delle modifiche apportate dal team AMS Accelerate Operations e dall'automazione di AMS Accelerate fornendo un'interfaccia interrogabile utilizzando la console Amazon Athena (Athena) e la gestione dei log di AMS Accelerate.

Athena è un servizio di query interattivo che puoi utilizzare per analizzare i dati in Amazon S3 utilizzando lo Structured Query Language (SQL) standard (vedi SQL Reference per Amazon Athena). Athena è un servizio serverless, perciò non occorre installare o gestire alcuna infrastruttura e vengono addebitati solo i costi relativi all'esecuzione delle query. AMS Accelerate crea tabelle Athena con partizioni giornaliere sui CloudTrail log e fornisce query sulla AWS regione principale e all'interno del gruppo di lavoro. ams-change-record Puoi scegliere una qualsiasi delle query predefinite ed eseguirle secondo necessità. Per ulteriori informazioni sui gruppi di lavoro Athena, consulta Come funzionano i gruppi di lavoro.

> **Note**
>
> Solo Accelerate può interrogare CloudTrail gli eventi per il tuo account Accelerate utilizzando Athena quando Accelerate è integrato con il percorso CloudTrail dell'organizzazione, a meno che l'amministratore dell'organizzazione non abbia implementato un ruolo IAM per utilizzare Athena per interrogare e analizzare CloudTrail gli eventi nel tuo account, durante l'onboarding.

Utilizzando change record, puoi rispondere facilmente a domande come:

- Chi (AMS Accelerate Systems o AMS Accelerate Operators) ha avuto accesso al tuo account
- Quali modifiche sono state apportate da AMS Accelerate al tuo account
- Quando AMS Accelerate ha apportato modifiche al tuo account
- A chi rivolgerti per visualizzare le modifiche apportate al tuo account
- Perché AMS Accelerate aveva bisogno di apportare le modifiche al tuo account
- Come modificare le query per ottenere risposte a tutte quelle domande anche per eventuali modifiche non relative ad AMS

Visualizzazione dei record delle modifiche

Per utilizzare le query Athena, accedi alla console di AWS gestione e accedi alla console Athena nella tua regione principale. AWS

> **Note**
>
> Se vedi la pagina Get Started di Amazon Athena mentre esegui uno dei passaggi, fai clic su Inizia. Questo potrebbe apparire anche se la tua infrastruttura Change Record è già attiva.

1. Scegli Workgroup dal pannello di navigazione superiore della console Athena.
2. Scegli il ams-change-recordgruppo di lavoro, quindi fai clic su Cambia gruppo di lavoro.
3. Scegliete ams-change-record-databasedalla casella combinata Database. ams-change-record-databaseInclude la ams-change-record-tabletabella.
4. Scegli Query salvate dal pannello di navigazione superiore.
5. La finestra Interrogazioni salvate mostra un elenco di interrogazioni fornite da AMS Accelerate, che puoi eseguire. Scegli la query che desideri eseguire dall'elenco delle interrogazioni salvate. Ad esempio, la query ams_session_accesses_v1.

   Per l'elenco completo delle query AMS Accelerate preimpostate, consulta. Interrogazioni predefinite
6. Se necessario, modifica il filtro datetime nella casella dell'editor di query; per impostazione predefinita, la query controlla solo le modifiche dell'ultimo giorno.
7. Scegli Esegui query.

Interrogazioni predefinite

AMS Accelerate fornisce diverse query predefinite che è possibile utilizzare all'interno della console Athena. Le interrogazioni predefinite sono elencate nelle seguenti tabelle.

> **Note**
>
> - Tutte le query accettano l'intervallo di data e ora come filtro opzionale; per impostazione predefinita, tutte le query vengono eseguite nelle ultime 24 ore. Per l'input previsto, vedere la seguente sottosezione,. Modifica del filtro datetime nelle query
> - Gli input dei parametri che è possibile o necessario modificare vengono visualizzati nella query come nel caso delle parentesi *<PARAMETER_NAME>* angolari. Sostituite il segnaposto e le parentesi angolari con il valore del parametro.

- Tutti i filtri sono opzionali. Nelle query, alcuni filtri opzionali sono commentati con un doppio trattino (--) all'inizio della riga. Tutte le query verranno eseguite senza di essi, con parametri predefiniti. Se desideri specificare i valori dei parametri per questi filtri opzionali, rimuovi il doppio trattino (--) all'inizio della riga e sostituisci il parametro come desideri.
- Tutte le interrogazioni restituiscono `IAM PincipalId` e `IAM SessionId` negli output
- Il costo calcolato per l'esecuzione di una query dipende dal numero di CloudTrail log generati per l'account. Per calcolare il costo, utilizza il calcolatore dei prezzi di AWS Athena.

Query predefinite

Scopo/descrizione	Input	Output
Nome della query: `ams_access_session_query_v1`		
Tracciamento delle sessioni di accesso con AMS Fornisce informazioni su una sessione di accesso AMS Accelerate specifica. La query accetta l'IAM Principal ID come filtro opzionale e restituisce l'ora dell'evento, le esigenze aziendali di accesso all'account, il richiedente e così via. Puoi filtrare in base a uno specifico IAM Principal ID decommentando la riga e sostituendo il segnaposto *`IAM PrincipalId`* con un ID specifico nell'editor di query.	(Facoltativo)`IAM PrincipalId` : l'identificatore principale IAM della risorsa a cui sta tentando di accedere. Il formato è*`UNIQUE_ID ENTIFIER`* :*`RESOURCE_NAME`* . Per i dettagli, vedere gli identificatori univoci. Puoi eseguire la query senza questo filtro per determinare lo IAM PrincipalId esatto con cui desideri filtrare.	• EventTime: Ora di ottenimento dell'accesso • EventName: nome evento AWS (AssumeRole) • EventRegion: Regione AWS che riceve la richiesta • EventId: ID CloudTrail evento • BusinessNeed Tipo: tipo di motivo aziendale per accedere all'account. I valori consentiti sono: SupportCase, OpsItem, Issue, Text. • BusinessNeed: L'azienda deve accedere all'account. Ad esempio, Support Case ID, Ops Item ID e così via. • Richiedente: ID operatore che accede all'account o sistema di automazione che accede all'account.

Scopo/descrizione	Input	Output
Puoi anche elencare le sessioni di accesso non AMS rimuovendo la riga del filtro useragent nella clausola WHERE della query.		• RequestAccessType: Tipo di richiedente (System, OpsAPI OpsConsole, Unset)
Nome della query: `ams_events_query_v1`		
Tieni traccia di tutte le azioni di mutazione eseguite da AMS Accelerate Restituisce tutte le azioni di scrittura eseguite sull'account utilizzando quel filtro di ruolo AMS Accelerate. Puoi anche tenere traccia delle azioni di mutazione eseguite da ruoli non AMS rimuovendo le righe del filtro useridentity.arn dalla clausola WHERE della query.	(Facoltativo) Solo intervallo di data/ora. Per informazioni, consulta Modifica del filtro datetime nelle query.	• AccountId: ID account AWS • RoleArn: RoleArn per il richiedente • EventTime: Ora di ottenimento dell'accesso • EventName: nome evento AWS (AssumeRole) • EventRegion: Regione AWS che riceve la richiesta • EventId: ID CloudTrail evento • RequestParameters : parametri di richiesta per la richiesta • ResponseElements: elementi di risposta per la risposta. • UserAgent: Agente CloudTrail utente AWS
Nome della query: `ams_instance_access_sessions_query_v1`		

Scopo/descrizione	Input	Output
Tieni traccia degli accessi alle istanze tramite AMS Accelerate Restituisce un elenco di accessi alle istanze AMS Accelerate; ogni record include l'ora dell'evento, la regione dell'evento, l'ID dell'istanza, l'ID principal e IAM, l'ID della sessione IAM, l'ID della sessione SSM. Puoi utilizzare l'IAM Principal ID per ottenere maggiori dettagli sulle esigenze aziendali di accesso all'istanza utilizzando la query `ams_access_sessions_query_v1` Athena. Puoi utilizzare l'ID di sessione SSM per ottenere maggiori dettagli sulla sessione di accesso all'istanza, tra cui l'ora di inizio e di fine della sessione, i dettagli del registro e l'utilizzo della console di AWS Session Manager nella regione dell' AWS istanza. Gli utenti possono anche elencare gli accessi alle istanze non AMS	Solo `datetime range`. Per informazioni, consulta Modifica del filtro datetime nelle query.	• InstanceId: ID dell'istanza • SSMSession Id: ID sessione SSM • RoleArn: RoleArn per il richiedente • EventTime: Ora di ottenimento dell'accesso • EventName: nome evento AWS (AssumeRole) • EventRegion: Regione AWS che riceve la richiesta • EventId: ID CloudTrail evento

Scopo/descrizione	Input	Output
rimuovendo la riga del filtro useridentity nella clausola WHERE della query.		
Nome della query: ams_privilege_escalation_events_query_v1		

Scopo/descrizione	Input	Output
Tieni traccia degli eventi di autorizzazione (escalation) per utenti AMS e non AMS Fornisce un elenco di eventi che possono portare direttamente o potenzialmente a un'escalation dei privilegi. La query viene ActionedBy accettata come filtro opzionale e restituisce EventName, EventId EventTime, e così via. Vengono inoltre restituiti tutti i campi associati all'evento. I campi sono vuoti se non applicabili per quell'evento. Per impostazione predefinita, il ActionedBy filtro è disabilitato; per attivarlo, rimuovi «--" da quella riga. Per impostazione predefinita, il ActionedBy filtro è disabilitato (mostrerà gli eventi di escalation dei privilegi di tutti gli utenti). Per mostrare gli eventi per un particolare utente o ruolo, rimuovi il doppio	(Facoltativo)`ACTIONEDBY_PUT_USER_NAME` : nome utente per l'utente ActionedBy. Può trattarsi di un utente o di un ruolo IAM. Ad esempio,. ams-access-admin (Facoltativo)`datetime range`. Per informazioni, consulta Modifica del filtro datetime nelle query.	• AccountId: ID dell'account • ActionedBy: ActionedBy Nome utente • EventTime: Ora di ottenimento dell'accesso • EventName: nome dell'evento AWS (AssumeRole). • EventRegion: Regione AWS che riceve la richiesta • EventId: ID CloudTrail evento

Scopo/descrizione	Input	Output
trattino (--) dalla riga del filtro useridentity nella clausola WHERE e sostituisci il segnaposto *ACTIONEDBY_PUT_USER_NAME_HERE* con un nome utente o di ruolo IAM. Puoi eseguire la query senza il filtro per determinare l'utente esatto con cui desideri filtrare.		
Nome della query: ams_resource_events_query_v1		
Tieni traccia degli eventi di scrittura per risorse specifiche (AMS o non AMS) Fornisce un elenco di eventi eseguiti su una risorsa specifica . La query accetta l'ID della risorsa come parte dei filtri (sostituisci il segnaposto *RESOURCE_INFO* nella clausola WHERE della query) e restituisce tutte le azioni di scrittura eseguite su quella risorsa.	(Obbligatorio)RESOURCE_INFO : l'identificatore di risorsa può essere un ID per qualsiasi risorsa AWS nell'acco unt. Non confonderlo con una risorsa. ARNs Ad esempio, un ID di istanza per un' EC2 istanza, un nome di tabella per una tabella DynamoDB logGroupName , per CloudWatch un registro, ecc. (Facoltativo). datetime range Per informazioni, consulta Modifica del filtro datetime nelle query.	• AccountId: ID dell'account • ActionedBy: ActionedBy Nome utente • EventTime: Ora di ottenimento dell'accesso • EventName: nome dell'evento AWS (AssumeRole). • EventRegion: Regione AWS che riceve la richiesta • EventId: ID CloudTrail evento
Nome della query: ams_session_events_query_v1		

Scopo/descrizione	Input	Output
Tieni traccia delle azioni di scrittura eseguite da AMS Accelerate durante una sessione specifica Fornisce un elenco di eventi eseguiti in una sessione specifica. La query accetta l'ID principale IAM come parte dei filtri (sostituisce il segnaposto *PRINCIPAL_ID* nella clausola WHERE della query) e restituisce tutte le azioni di scrittura eseguite su quella risorsa.	(Obbligatorio)`PRINCIPAL_ID` : ID principal e per la sessione. Il formato è*UNIQUE_ID ENTIFIER* :*RESOURCE_NAME* . Per i dettagli, vedere gli identificatori univoci. Puoi eseguire la query «ams_session_ids_by_requester_v1" per ottenere l'elenco degli IAM Principal per un richiedente. IDs Puoi anche eseguire la query senza questo filtro per determinare l'esatto IAM con cui desideri filtrare. PrincipalId (Facoltativo)`datetime range`. Per informazioni, consulta Modifica del filtro datetime nelle query.	• AccountId: ID dell'account • ActionedBy: ActionedBy Nome utente • EventTime: Ora di ottenimento dell'accesso • EventName: nome evento AWS (AssumeRole) • EventRegion: Regione AWS che riceve la richiesta • EventId: ID CloudTrail evento
Nome della query: `ams_session_ids_by_requester_v1`		

Scopo/descrizione	Input	Output
Tieni traccia di IAM Principal/Session IDs per un richiedente specifico. La query accetta «richiedente» (sostitui sce il segnaposto *Requester* nella clausola WHERE della query) e restituisce tutti gli ID principali IAM di quel richiedente durante l'intervallo di tempo specificato.	(Obbligatorio)`Requester` : ID operatore che accede all'account (ad esempio: alias di un operatore) o sistema di automazione che accede all'account (ad esempio:, , ecc.). OsConfiguration AlarmManager (Facoltativo). `datetime range` Per informazioni, consulta Modifica del filtro datetime nelle query.	• IAM PrincipalId - IAM Principal ID della sessione. Il formato è*UNIQUE_ID ENTIFIER* :*RESOURCE_NAME* . Per i dettagli, vedere gli identificatori univoci. Puoi eseguire la query senza questo filtro per determinare lo IAM esatto con PrincipalId cui desideri filtrare. • IAM SessionId : ID di sessione IAM per la sessione di accesso • EventTime: Ora di ottenimento dell'accesso

Modifica del filtro datetime nelle query

Tutte le query accettano l'intervallo di data e ora come filtro opzionale. Per impostazione predefinita, tutte le query vengono eseguite nell'ultimo giorno.

Il formato utilizzato per il campo datetime è yyyy/MM/dd (ad esempio: 01/01/2021). Ricorda che memorizza solo la data e non l'intero timestamp. Per l'intero timestamp, usa il campo eventime, che memorizza il timestamp nel formato ISO 8601 yyyy-MM-dd T HH:mm:ss Z (ad esempio: 2021-01-01T 23:59:59 Z). Tuttavia, poiché la tabella è partizionata nel campo datetime, dovrai passare sia il filtro datetime che il filtro eventtime alla query. Fare riferimento agli esempi riportati di seguito.

> **Note**
>
> Per vedere tutti i modi accettati per modificare l'intervallo, consulta l'ultima documentazione delle funzioni Presto basata sulla versione del motore Athena attualmente utilizzata per le funzioni e gli operatori di data e ora per vedere tutti i modi accettati per modificare l'intervallo.

Livello di data: Ultimo giorno o ultime 24 ore (impostazione predefinita) Esempio: se CURRENT_DATE='2021/01/01', il filtro sottrarrà un giorno dalla data corrente e la formatterà come datetime > '2020/12/31'

```
datetime > date_format(date_add('day', - 1, CURRENT_DATE), '%Y/%m/%d')
```

Livello di data: esempio degli ultimi 2 mesi:

```
datetime > date_format(date_add('month', - 2, CURRENT_DATE), '%Y/%m/%d')
```

Livello di data: esempio tra 2 date:

```
datetime > '2021/01/01'
      AND
      datetime < '2021/01/10'
```

Livello di timestamp: esempio delle ultime 12 ore:

Suddividi i dati in modo che durino 1 giorno, quindi filtra tutti gli eventi delle ultime 12 ore

```
datetime > date_format(date_add('day', - 1, CURRENT_DATE), '%Y/%m/%d')
      AND
      eventtime > date_format(date_add('hour', - 12, CURRENT_TIMESTAMP), '%Y-%m-%dT%H:
%i:%sZ')
```

Livello di timestamp: tra 2 timestamp. Esempio:

Ricevi eventi tra le 12:00 del 1 gennaio 2021 e le 15:00 del 10 gennaio 2021.

```
datetime > '2021/01/01' AND datetime < '2021/01/10'
      AND
      eventtime > '2021-01-01T12:00:00Z' AND eventtime < '2021-01-10T15:00:00Z'
```

Esempi di query predefiniti

ams_access_session_query_v1

```
Name: ams_access_session_query_v1

Description: >-
   The query provides more information on specific AMS access session.
```

```
    The query accepts IAM Principal Id as an optional filter and returns event time,
  business need for accessing the account, requester, ... etc.
    By default; the query filter last day events only, the user can change the datetime
  filter to search for more wide time range.
    By default; the IAM PrincipalId filter is disabled. To enable it, remove "-- " from
  that line.

AthenaQueryString: |-
    /*
      The query provides list of AMS access sessions during specific time range.
      The query accepts IAM Principal Id as an optional filter and returns event time,
  business need for accessing the account, requester, ... etc.

      By default, the query filters the last day's events only; you can change the
  "datetime" filter to search for a wider time range.

      By default; the IAM Principal ID filter is disabled (it shows access sessions for
  all IAM principals).
      If you want to only show access sessions for a particular IAM principal ID, remove
  the double-dash (--) from
      the "IAM Principal ID" filter line in the WHERE clause of the query, and replace
  the placeholder "<IAM PrincipalId>" with the specific ID that you want.
      You can run the query without the filter to determine the exact IAM PrincipalId
  you want to filter with.

      By default; the query only shows AMS access sessions. If you also want to show
  non-AMS access sessions,
      remove the "useragent" filter in the WHERE clause of the query.

      For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
  in your AMS Accelerate accounts -> Default Queries
    */

    SELECT
       json_extract_scalar(responseelements, '$.assumedRoleUser.assumedRoleId') AS "IAM
  PrincipalId",
       json_extract_scalar(responseelements, '$.credentials.accessKeyId') AS "IAM
  SessionId",
       eventtime AS "EventTime",
       eventname AS "EventName",
       awsregion AS "EventRegion",
       eventid AS "EventId",
       json_extract_scalar(requestparameters, '$.tags[0].value') AS "BusinessNeed",
       json_extract_scalar(requestparameters, '$.tags[1].value') AS "BusinessNeedType",
```

```
      json_extract_scalar(requestparameters, '$.tags[2].value') AS "Requester",
      json_extract_scalar(requestparameters, '$.tags[3].value') AS "AccessRequestType"
   FROM
       "{DATABASE NAME HERE}".{TABLENAME HERE} <- This should auto-populate
   WHERE
      datetime > date_format(date_add('day', - 1, CURRENT_DATE), '%Y/%m/%d')
      AND eventname = 'AssumeRole'
      AND useragent = 'access.managedservices.amazonaws.com'
      -- AND  json_extract_scalar(responseelements, '$.assumedRoleUser.assumedRoleId')
 = '<IAM PrincipalId>'
   ORDER BY eventtime

InsightsQueryString: |-
   # The query provides list of AMS access sessions during specific time range.
   # The query accepts IAM Principal Id as an optional filter and returns event time,
 business need for accessing the account, requester, ... etc.
   #
   # By default; the IAM Principal ID filter is disabled (it shows access sessions for
 all IAM principals).
   # If you want to only show access sessions for a particular IAM principal ID, remove
 the # (#) from
   # the "IAM Principal ID" filter of the query, and replace the placeholder "<IAM
 PrincipalId>" with the specific ID that you want.
   # You can run the query without the filter to determine the exact IAM PrincipalId
 you want to filter with.
   #
   # By default; the query only shows AMS access sessions. If you also want to show
 non-AMS access sessions,
   # remove the "useragent" filter from the query.
   #
   # For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
 in your AMS Accelerate accounts -> Default Queries

   filter eventName="AssumeRole" AND userAgent="access.managedservices.amazonaws.com"
   # | filter responseElements.assumedRoleUser.assumedRoleId= "<IAM PrincipalId>"
   | sort eventTime desc
   | fields
      responseElements.assumedRoleUser.assumedRoleId as IAMPrincipalId,
      responseElements.credentials.accessKeyId as IAMSessionId,
      eventTime as EventTime,
      eventName as EventName,
      awsRegion as EventRegion,
      eventID as EventId,
      requestParameters.tags.0.value as BusinessNeed,
```

```
      requestParameters.tags.1.value as BusinessNeedType,
      requestParameters.tags.2.value as Requester,
      requestParameters.tags.3.value as AccessRequestType
```

ams_events_query_v1

```
ams_events_query_v1.yaml
/*
  The query provides list of events to track write actions for all AMS changes.
  The query returns all write actions done on the account using that AMS role filter.

  By default, the query filters the last day's events only; you can change the
 "datetime" filter to search for a wider time range.

  You can also track mutating actions done by non-AMS roles by removing the
 "useridentity.arn" filter lines from the WHERE clause of the query.

  For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes in
 your AMS Accelerate accounts -> Default Queries
*/

SELECT
   useridentity.principalId AS "IAM PrincipalId",
   useridentity.accesskeyid AS "IAM SessionId",
   useridentity.accountid AS "AccountId",
   useridentity.arn AS "RoleArn",
   eventid AS "EventId",
   eventname AS "EventName",
   awsregion AS "EventRegion",
   eventsource AS "EventService",
   eventtime AS "EventTime",
   requestparameters As "RequestParameters",
   responseelements AS "ResponseElements",
   useragent AS "UserAgent"
FROM
   "{DATABASE NAME HERE}".{TABLENAME HERE} <- This should auto-populate
WHERE
   readonly <> 'true'
   AND
   (
      LOWER(useridentity.arn) LIKE '%/ams%'
      OR LOWER(useridentity.arn) LIKE '%/customer_ssm_automation_role%'
```

```
   )
ORDER BY eventtime
```

ams_instance_access_sessions_query_v1

```
ams_instance_access_sessions_query_v1
/*
  The query provides list of AMS Instance accesses during specific time range.

  The query returns the list of AMS instance accesses; every record includes the event
 time, the event AWS Region, the instance ID, the IAM session ID, and the SSM session
 ID.
  You can use the IAM Principal ID to get more details on the business need for
 accessing the instance by using ams_access_session_query_v1 athena query.
  You can use the SSM session ID to get more details on the instance access session,
 including the start and end time of the session and log details, using the AWS Session
 Manager Console in the instance's AWS Region.

  You can also list non-AMS instance accesses by removing the "useridentity" filter
 line in the WHERE clause of the query.

  By default, the query filters the last day's events only; you can change the
 "datetime" filter to search for a wider time range.

  For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes in
 your AMS Accelerate accounts -> Default Queries
*/

SELECT
   useridentity.principalId AS "IAM PrincipalId",
   useridentity.accesskeyid AS "IAM SessionId",
   json_extract_scalar(requestparameters, '$.target') AS "InstanceId",
   json_extract_scalar(responseelements, '$.sessionId') AS "SSM SessionId",
   eventname AS "EventName",
   awsregion AS "EventRegion",
   eventid AS "EventId",
   eventsource AS "EventService",
   eventtime AS "EventTime"
FROM
   "{DATABASE NAME HERE}".{TABLENAME HERE} <- This should auto-populate
WHERE
   useridentity.sessionContext.sessionIssuer.arn like '%/ams_%'
   AND eventname = 'StartSession'
```

```
ORDER BY eventtime
```

ams_privilege_escalation_events_query_v1

```
ams_privilege_escalation_events_query_v1.yaml
/*
  The query provides list of events that can directly or potentially lead to a
 privilege escalation.

  The query accepts ActionedBy as an optional filter and returns EventName, EventId,
 EventTime, ... etc.
  All fields associated with the event are also returned. Some fields are blank if not
 applicable for that event.
  You can use the IAM Session ID to get more details about events happened in that
 session by using ams_session_events_query_v1 query.

  By default, the query filters the last day's events only; you can change the
 "datetime" filter to search for a wider time range.

  By default, the ActionedBy filter is disabled (it shows privilege escalation events
 from all users).
  To show events for a particular user or role, remove the double-dash (--) from the
 useridentity filter line in the WHERE clause of the query
  and replace the placeholder "<ACTIONEDBY_PUT_USER_NAME_HERE>" with an IAM user or
 role name.
  You can run the query without the filter to determine the exact user you want to
 filter with.

  For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes in
 your AMS Accelerate accounts -> Default Queries
*/

SELECT
   useridentity.principalId AS "IAM PrincipalId",
   useridentity.accesskeyid AS "IAM SessionId",
   useridentity.accountid AS "AccountId",
   reverse(split_part(reverse(useridentity.arn), ':', 1)) AS "ActionedBy",
   eventname AS "EventName",
   awsregion AS "EventRegion",
   eventid AS "EventId",
   eventtime AS "EventTime",
   json_extract_scalar(requestparameters, '$.userName') AS "UserName",
   json_extract_scalar(requestparameters, '$.roleName') AS "RoleName",
```

```
   json_extract_scalar(requestparameters, '$.groupName') AS "GroupName",
   json_extract_scalar(requestparameters, '$.policyArn') AS "PolicyArn",
   json_extract_scalar(requestparameters, '$.policyName') AS "PolicyName",
   json_extract_scalar(requestparameters, '$.permissionsBoundary') AS
 "PermissionsBoundary",
   json_extract_scalar(requestparameters, '$.instanceProfileName') AS
 "InstanceProfileName",
   json_extract_scalar(requestparameters, '$.openIDConnectProviderArn') AS
 "OpenIDConnectProviderArn",
   json_extract_scalar(requestparameters, '$.serialNumber') AS "SerialNumber",
   json_extract_scalar(requestparameters, '$.serverCertificateName') AS
 "ServerCertificateName",
   json_extract_scalar(requestparameters, '$.accessKeyId') AS "AccessKeyId",
   json_extract_scalar(requestparameters, '$.certificateId') AS "CertificateId",
   json_extract_scalar(requestparameters, '$.newUserName') AS "NewUserName",
   json_extract_scalar(requestparameters, '$.newGroupName') AS "NewGroupName",
   json_extract_scalar(requestparameters, '$.newServerCertificateName') AS
 "NewServerCertificateName",
   json_extract_scalar(requestparameters, '$.name') AS "SAMLProviderName",
   json_extract_scalar(requestparameters, '$.sAMLProviderArn') AS "SAMLProviderArn",
   json_extract_scalar(requestparameters, '$.sSHPublicKeyId') AS "SSHPublicKeyId",
   json_extract_scalar(requestparameters, '$.virtualMFADeviceName') AS
 "VirtualMFADeviceName"
FROM
   "{DATABASE NAME HERE}".{TABLENAME HERE} <- This should auto-populate
WHERE
   (
     -- More event names can be found at https://docs.aws.amazon.com/IAM/latest/
UserGuide/list_identityandaccessmanagement.html
     eventname LIKE 'Add%' OR
     eventname LIKE 'Attach%' OR
     eventname LIKE 'Delete%' AND eventname != 'DeleteAccountAlias' OR
     eventname LIKE 'Detach%' OR
     eventname LIKE 'Create%' AND eventname != 'CreateAccountAlias' OR
     eventname LIKE 'Put%' OR
     eventname LIKE 'Remove%' OR
     eventname LIKE 'Update%' OR
     eventname LIKE 'Upload%' OR
     eventname = 'DeactivateMFADevice' OR
     eventname = 'EnableMFADevice' OR
     eventname = 'ResetServiceSpecificCredential' OR
     eventname = 'SetDefaultPolicyVersion'
   )
   AND eventsource = 'iam.amazonaws.com'
```

```
ORDER BY eventtime
```

ams_resource_events_query_v1

```
Name: ams_resource_events_query_v1

Description: >-
   The query provides list of events done on specific resource.
   The query accepts resource id as part of the filters, and return all write actions
 done on that resource.
   By default; the query list the accesses for last day, the user can change the time
 range by changing the datetime filter.

AthenaQueryString: |-
   /*
     The query provides list of events done on specific resource.

     The query accepts the resource ID as part of the filters (replace the placeholder
 "<RESOURCE_INFO>" in the WHERE clause of the query),
     and returns all write actions done on that resource. The resource ID can be an ID
 for any AWS resource in the account.
     Example: An instance ID for an EC2 instance, table name for a DynamoDB table,
 logGroupName for a CloudWatch Log, etc.

     By default, the query filters the last day's events only; you can change the
 "datetime" filter to search for a wider time range.

     For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
 in your AMS Accelerate accounts -> Default Queries
   */

   SELECT
      useridentity.principalId AS "IAM PrincipalId",
      useridentity.accesskeyid AS "IAM SessionId",
      useridentity.accountid AS "AccountId",
      reverse(split_part(reverse(useridentity.arn), ':', 1)) AS "ActionedBy",
      eventname AS "EventName",
      awsregion AS "EventRegion",
      eventid AS "EventId",
      eventsource AS "EventService",
      eventtime AS "EventTime"
   FROM
       "{DATABASE NAME HERE}".{TABLENAME HERE} <- This should auto-populate
```

```
   WHERE
      datetime > date_format(date_add('day', - 1, CURRENT_DATE), '%Y/%m/%d')
      AND readonly <> 'true'
      AND
      (
         requestparameters LIKE '%<RESOURCE_INFO>%'
         OR responseelements LIKE '%<RESOURCE_INFO>%'
      )
   ORDER BY eventtime

InsightsQueryString: |-
   # The query provides list of events done on specific resource.
   #
   # The query accepts the resource ID as part of the filters (replace the placeholder
 "<RESOURCE_INFO>" in the filter of the query),
   # and returns all write actions done on that resource. The resource ID can be an ID
 for any AWS resource in the account.
   # Example: An instance ID for an EC2 instance, table name for a DynamoDB table,
 logGroupName for a CloudWatch Log, etc.
   #
   # For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
 in your AMS Accelerate accounts -> Default Queries

   filter readOnly=0
   | parse @message '"requestParameters":{*}' as RequestParameters
   | parse @message '"responseElements":{*}' as ResponseElements
   # | filter RequestParameters like "RESOURCE_INFO" or ResponseElements like
 "<RESOURCE_INFO>"
   | fields
      userIdentity.principalId as IAMPrincipalId,
      userIdentity.accessKeyId as IAMSessionId,
      userIdentity.accountId as AccountId,
      userIdentity.arn as ActionedBy,
      eventName as EventName,
      awsRegion as EventRegion,
      eventID as EventId,
      eventSource as EventService,
      eventTime as EventTime
   | display IAMPrincipalId, IAMSessionId, AccountId, ActionedBy, EventName,
 EventRegion, EventId, EventService, EventTime
   | sort eventTime desc
```

ams_session_events_query_v1

```
Name: ams_session_events_query_v1

Description: >-
   The query provides list of events done on specific session.
   The query accepts IAM Principal Id as part of the filters, and return all write
 actions done on that resource.
   By default; the query list the accesses for last day, the user can change the time
 range by changing the datetime filter.

AthenaQueryString: |-
   /*
     The query provides a list of events executed on a specific session.

     The query accepts the IAM principal ID as part of the filters (replace the
 placeholder "<PRINCIPAL_ID>" in the WHERE clause of the query),
     and returns all write actions done on that resource.

     By default, the query filters the last day's events only; you can change the
 "datetime" filter to search for a wider time range.

     For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
 in your AMS Accelerate accounts -> Default Queries
   */

   SELECT
      useridentity.principalId AS "IAM PrincipalId",
      useridentity.accesskeyid AS "IAM SessionId",
      useridentity.accountid AS "AccountId",
      reverse(split_part(reverse(useridentity.arn), ':', 1)) AS "ActionedBy",
      eventname AS "EventName",
      awsregion AS "EventRegion",
      eventsource AS "EventService",
      eventtime AS "EventTime",
      requestparameters As "RequestParameters",
      responseelements AS "ResponseElements",
      useragent AS "UserAgent"
   FROM
       "{DATABASE NAME HERE}".{TABLENAME HERE} <- This should auto-populate   WHERE
      useridentity.principalid = '<PRINCIPAL_ID>'
      AND datetime > date_format(date_add('day', - 1, CURRENT_DATE), '%Y/%m/%d')
      AND readonly <> 'true'
   ORDER BY eventtime
```

```
InsightsQueryString: |-
   # The query provides a list of events executed on a specific session.
   #
   # The query accepts the IAM principal ID as part of the filters (replace the
 placeholder "<PRINCIPAL_ID>" in the filter of the query),
   # and returns all write actions done on that resource.
   #
   # For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
 in your AMS Accelerate accounts -> Default Queries

   filter readOnly=0 AND userIdentity.principalId = "<IAM Principal>"
   | sort eventTime desc
   | fields
      userIdentity.accessKeyId as IAMSessionId,
      userIdentity.principalId as IAMPrincipalId,
      userIdentity.accountId as AccountId,
      userIdentity.arn as ActionedBy,
      eventName as EventName,
      awsRegion as EventRegion,
      eventSource as EventService,
      eventTime as EventTime,
      userAgent as UserAgent
   | parse @message '"requestParameters":{*}' as RequestParameters
   | parse @message '"responseElements":{*}' as ResponseElements
```

ams_session_ids_by_requester_v1

```
Name: ams_session_ids_by_requester_v1

Description: >-
   The query provides list of IAM Principal/Session Ids for specific requester.
   The query accepts requester and return all IAM Principal/Session Ids by that
 requester during specific time range.
   By default; the query list the accesses for last day, the user can change the time
 range by changing the datetime filter.

AthenaQueryString: |-
   /*
     The query provides list of IAM Principal IDs for a specific requester.

     The query accepts the requester (replace placeholder "<Requester>" in the WHERE
 clause of the query),
```

```
     and returns all IAM Principal IDs by that requester during a specific time range.

     By default, the query filters the last day's events only; you can change the
 "datetime" filter to search for a wider time range.

     For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
 in your AMS Accelerate accounts -> Default Queries
   */

   SELECT
      json_extract_scalar(responseelements, '$.assumedRoleUser.assumedRoleId') AS "IAM
 PrincipalId",
      json_extract_scalar(responseelements, '$.credentials.accessKeyId') AS "IAM
 SessionIId",
      eventtime AS "EventTime"
   FROM
       "{DATABASE NAME HERE}".{TABLENAME HERE} <- This should auto-populate
   WHERE
      datetime > date_format(date_add('day', - 1, CURRENT_DATE), '%Y/%m/%d')
      AND json_extract_scalar(requestparameters, '$.tags[2].value') = '<Requester>'
   ORDER BY eventtime

InsightsQueryString: |-
   # The query provides list of IAM Principal IDs for a specific requester.
   #
   # The query accepts the requester (replace placeholder "<Requester>" in the filter
 of the query),
   # and returns all IAM Principal IDs by that requester during a specific time range.
   #
   # For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
 in your AMS Accelerate accounts -> Default Queries
   filter eventName="AssumeRole" AND requestParameters.tags.2.value="<Requester>"
   | sort eventTime desc
   | fields
      responseElements.assumedRoleUser.assumedRoleId as IAMPrincipalId,
      responseElements.credentials.accessKeyId as IAMSessionId,
      eventTime as EventTime
```

Modificare le autorizzazioni di registrazione

Le seguenti autorizzazioni sono necessarie per eseguire le query di modifica dei record:

- Athena

  - atena: GetWorkGroup
  - atena: StartQueryExecution
  - atena: ListDataCatalogs
  - atena: GetQueryExecution
  - atena: GetQueryResults
  - atena: BatchGetNamedQuery
  - atena: ListWorkGroups
  - atena: UpdateWorkGroup
  - atena: GetNamedQuery
  - atena: ListQueryExecutions
  - atena: ListNamedQueries
- AWS KMS
  - kms:Decrypt
  - AWS KMS ID chiave di AMSCloudTrailLogManagement, o i tuoi ID AWS KMS chiave, se Accelerate utilizza il tuo archivio dati del bucket di eventi CloudTrail trail Amazon S3 utilizzando la crittografia SSE-KMS.
- AWS Glue
  - colla: GetDatabase
  - colla: GetTables
  - colla: GetDatabases
  - colla: GetTable
- Accesso in lettura ad Amazon S3
  - CloudTrail Datastore del bucket Amazon S3: ams-a *`AccountId`* -cloudtrail- o il nome del tuo bucket Amazon S3*`primary region`*, trail events Amazon S3 bucket data store. CloudTrail
- Accesso in scrittura ad Amazon S3
  - Risultati delle query sugli eventi Athena Bucket Amazon S3: ams-a athena-results- *`AccountId primary region`*

AWS Systems Manager in Accelerate

Un AWS Systems Manager documento (documento SSM) definisce le azioni che Systems Manager esegue sulle AWS risorse. Systems Manager include più di una dozzina di documenti preconfigurati che è possibile utilizzare specificando i parametri in fase di esecuzione. I documenti utilizzano JavaScript Object Notation (JSON) o YAML e includono passaggi e parametri specificati dall'utente.

AWS Managed Services (AMS) è un editore affidabile per documenti SSM. I documenti SSM di proprietà di AMS sono condivisi solo con account AMS integrati, iniziano sempre con un prefisso riservato (AWSManagedServices-*) e vengono visualizzati nella console Systems Manager, di proprietà di Amazon. Il processo AMS per lo sviluppo e la pubblicazione di documenti SSM segue le best practice di AWS e richiede diverse revisioni tra pari durante l'intero ciclo di vita del documento. Per ulteriori informazioni sulle best practice di AWS per la condivisione di documenti SSM, visita Best practice for shared SSM documents.

Documenti AMS Accelerate SSM disponibili

I documenti AMS Accelerate SSM sono disponibili esclusivamente per i clienti AMS Accelerate e vengono utilizzati per automatizzare il flusso di lavoro operativo per la gestione dell'account.

Per visualizzare i documenti AMS Accelerate SSM disponibili su: Console di gestione AWS

1. Apri la console di Systems Manager dalla console.AWS Systems Manager
2. Scegli Condiviso con me.
3. Nella barra di ricerca, filtra per prefisso del nome del documento, quindi Uguale e imposta il valore su Services-. AWSManaged

   Per AWS CLI istruzioni, consulta Utilizzo di documenti SSM condivisi.

Versioni dei documenti AMS Accelerate SSM

I documenti SSM supportano il controllo delle versioni. I documenti AMS Accelerate SSM non possono essere modificati dall'account del cliente e non possono essere ricondivisi. Sono gestiti e mantenuti centralmente da AMS Accelerate per gestire l'account.

I numeri di versione vengono incrementati con ogni aggiornamento del documento in una regione AWS specifica. Man mano che nuove regioni diventano disponibili, lo stesso contenuto del

documento in due regioni può avere numeri di versione diversi; questo è tipico e non significa che il loro comportamento sarà diverso. Se desideri confrontare due documenti AMS Accelerate SSM, ti consigliamo di confrontare i loro hash con: AWS CLI

```
aws ssm describe-document \
--name AWSManagedServices-DOCUMENTNAME \
--output text --query "Document.Hash"
```

Due documenti SSM sono identici se i loro hash corrispondono.

Prezzi di Systems Manager

Non vi è alcun costo associato all'accesso ai documenti AMS Accelerate SSM. Il costo di runtime varia in base al tipo di documento SSM, ai relativi passaggi e alla durata del runtime. Per ulteriori informazioni, consulta i AWS Systems Manager prezzi.

Guida per l'utente della cronologia dei documenti di AMS Accelerate

La tabella seguente descrive le modifiche importanti in ogni versione della Guida per l'utente di AMS Accelerate. Per ricevere notifiche sugli aggiornamenti di questa documentazione, è possibile iscriversi a un feed RSS.

Modifica	Descrizione	Data
Documentazione aggiornata di Alarm Manager per l'aggiornamento del piano di controllo	Documentazione aggiornata di Alarm Manager per riflettere la migrazione del piano di controllo completata nel febbraio 2026: • Accelerate Alarm Manager: rimosso l'avviso di limitazione regionale, aggiunto enfasi agli avvisi di configurazione e rimossa la dichiarazione temporale relativa alle modifiche che entrano in vigore • Accelerate Configuration profile: monitoring - È stata rimossa la dichiarazione contraddittoria relativa a ConfigurationID • Profilo di configurazione accelerato: sostituzione di pseudoparametri - Aggiunti pseudoparametri per nuovi tipi di risorse e descrizioni esistenti aggiornate per istanze e dischi EC2, domini	31 marzo 2026

	Elasticsearch ed Elastic Load Balancing • Accelera gli esempi di configurazione degli allarmi: la dimensione del percorso rimossa dall'esempio di allarme su disco Linux come parametro del percorso del disco non è più supportata per Linux • La pagina obsoleta «Visualizzazione del numero di risorse monitorate da Alarm Manager» è stata rimossa poiché la funzionalità di reporting era obsoleta con l'aggiornamento del piano di controllo • Inventario delle risorse per Accelerate: aggiornato per fare riferimento al nuovo file di inventario delle risorse che riflette le modifiche all'architettura del piano di controllo	
Inventario delle risorse aggiornato per Accelerate	Sono stati aggiunti dettagli sul controllo della conformità dell'infrastruttura AMS.	27 marzo 2026
Raccomandazioni Compute Optimizer aggiornate (valori booleani)	Sono stati aggiornati tutti i valori dei parametri booleani da uppercase () per garantire la coerenza con le convenzioni standard. True/False) to lowercase (true/false	24 marzo 2026

Aggiornamento del punto 6.11 di AMS-STD-002 per le politiche relative a più account	È stato chiarito che le politiche tra account con accesso in scrittura agli account di terze parti possono essere configura te con l'accettazione del rischio.	24 marzo 2026
Note di AWS Health monitorag gio aggiornate	Ha chiarito che le notifiche vengono inviate solo per AWS Health gli eventi che richiedono l'intervento di AMS Operations.	24 marzo 2026
Aggiunta la correzione automatica della capacità del volume ONTAP	È stato aggiunto un AMSFSXONTAPVolume CapacityUtilization avviso alla tabella di riparazione automatica e è stata aggiunta una nuova sezione che descrive l'automazione della riparazione della capacità dei volumi ONTAP.	24 marzo 2026
Etichetta del campo relativa ai periodi di pianificazione di Resource Scheduler aggiornat a	È stata corretta l'etichetta del campo da «Pianificazioni» a «Periodi» nella procedura di aggiunta della pianificazione.	11 marzo 2026
Avvisi aggiornati dal monitorag gio di base nella sezione AMS	Avvisi aggiornati dal monitorag gio di base nella tabella AMS con condizione di attivazio ne aggiornata per l'istanza Amazon EC2: tutto. OSs	22 gennaio 2026

Sezione aggiornata del processo di Customer Security Risk Management	Sezione aggiornata del processo di Customer Security Risk Management con informazioni sull'accettazione del rischio, sulla validità, sulla revisione e sulla rinuncia.	15 gennaio 2026
Aggiornamento della sezione di automazione della correzione degli eventi a basso livello di storage di Amazon RDS in AMS (correzione automatica degli avvisi)	È stata aggiornata la sezione Amazon RDS sull'automazione della correzione degli eventi a basso livello di storage con informazioni sulle proprietà modificate dalle correzioni a seconda di un evento di attivazione.	15 gennaio 2026
Tabella aggiornata per la sezione Operations On Demand	È stata aggiornata la tabella per la sezione Operations On Demand con contenuti aggiornati.	7 gennaio 2026
Aggiornato e aggiunto nuovo contenuto a Trusted Remediator nella sezione AMS con informazioni su Security Hub CSPM	Ha aggiornato Trusted Remediator nella sezione AMS con informazioni su Security Hub CSPM e ha aggiunto una nuova pagina, i consigli CSPM di Security Hub supportati da Trusted Remediator.	11 dicembre 2025

Regioni supportate aggiornate	Sono state aggiunte note nelle seguenti sezioni relative ai servizi non disponibili nella regione Asia Pacifico (Malesia) : • Monitoraggio con Amazon Macie • Monitoraggio e gestione degli incidenti per Amazon EKS in AMS Accelerate • Installazione automatica di SSM Agent • Accelera Alarm Manager	24 ottobre 2025
Gestione dei log aggiornata — sezione AWS CloudTrail	Nuove informazioni e note relative alla AWS CloudTrail registrazione.	25 settembre 2025

Aggiunti 4 nuovi controlli di ottimizzazione dei Trusted Advisor costi supportati da Trusted Remediator	Sono stati aggiunti i seguenti controlli di ottimizzazione dei costi: • c1z7kmr00n - Raccomand azioni per l'ottimizzazione dei costi di Amazon EC2 per le istanze • c1z7kmr02n - Raccomand azioni per l'ottimizzazione dei costi di Amazon EBS per i volumi • c1z7kmr03n - Consigli per l'ottimizzazione dei costi di Amazon RDS per le istanze DB • c1z7kmr05n - AWS Lambda consigli per l'ottimizzazione dei costi per le funzioni	22 settembre 2025
Nota di deprecazione aggiornata per il servizio Change Record	Nota di deprecazione aggiornata per il servizio Change Record con soluzioni alternative.	11 settembre 2025
Controlli di Trusted Advisor sicurezza aggiornati supportati da Trusted Remediator	Aggiornati i parametri e i vincoli preconfigurati supportat i per il controllo Hs4Ma3G108: i trail devono essere integrati con Amazon Logs CloudTrail CloudWatch	5 settembre 2025

Controlli Trusted Advisor di sicurezza aggiornati supportati da Trusted Remediator	Controllo Trusted Advisor di sicurezza aggiornato per aggiungere la versione 2 di Hs4Ma3G184: la registrazione di Application Load Balancers e Classic Load Balancers deve essere abilitata	5 settembre 2025
Controlli di eccellenza Trusted Advisor operativa aggiornat i supportati dalla sezione Trusted Remediator	Controlli di eccellenza Trusted Advisor operativa aggiornat i supportati da Trusted Remediator per aggiungere un nuovo controllo supportat o c1fd6b96l4 Amazon S3 Access Logs Enabled.	28 agosto 2025
Sezione Trusted Remediato r aggiornata per includere nuovi contenuti per Compute Optimizer	Sezione Trusted Remediato r aggiornata per includere nuovi contenuti per i consigli supportati. AWS Compute Optimizer	18 agosto 2025
Link al glossario TOC rimosso	AWS Glossario.	8 agosto 2025
Link al glossario TOC rimosso	AWS Glossario.	8 agosto 2025
Nuovo campo nel rapporto Patch Daily	Tag dell'istanza: i tag associati all'ID dell'istanza Amazon EC2.	8 agosto 2025

Nuovi controlli Trusted Remediator	Trusted Advisor controlli di ottimizzazione dei costi supportati dai controlli di Trusted Advisor sicurezza Trusted Remediator supportati da Trusted Remediator Hs4Ma3G120— AWSManagedServices-TerminateEC2InstanceStoppedForPeriodOfTime, Hs4Ma3G230— 2 e c18d2gz150— 2. AWSManagedServices-TrustedRemediatorEnableBucketAccessLoggingV AWSManagedServices-TerminateEC InstanceStoppedForPeriodOfTime	8 agosto 2025
Aggiornamento dello standard IAM al punto 3.2	Linguaggio chiarito e rimossa la menzione dei tag.	25 luglio 2025
Profili di configurazione Resource Tagger aggiornati in Accelerate	Aggiunto un nuovo AvailabilityZone filtro nei profili di configurazione di Resource Tagger in Accelerate.	25 luglio 2025
Rapporti sugli incidenti, richieste di assistenza e domande di fatturazione aggiornati in Accelerate.	I riferimenti ai livelli di servizio Plus e Premium sono stati sostituiti con un collegamento allo SLA del servizio.	25 luglio 2025
Gestione aggiornata degli incidenti in Accelerate.	Informazioni aggiornate sui centri operativi.	25 luglio 2025
Pagina dei modelli AMS aggiornata con collegamenti corretti.	Sono stati corretti i collegamenti SLA e SLO.	25 luglio 2025

Aggiornamento delle opzioni di disattivazione degli avvisi	L'aggiunta di un tag consente di disattivare altri due avvisi.	25 luglio 2025
Nuova funzionalità per i backup	Personalizza le notifiche sugli archivi di backup con un nuovo tag.	25 luglio 2025
Sezione aggiornata per le configurazioni supportate in Accelerate	Configurazioni supportat e aggiornate per i sistemi operativi supportati e i sistemi operativi Supported End of Support (EOS) in Accelerate.	26 giugno 2025
Pagina rimossa Gestione dei tag per la gestione delle patch in Accelerate	Pagina rimossa Gestione dei tag per la gestione delle patch in Accelerate poiché questa funzionalità è obsoleta.	19 giugno 2025
Importante nota di sicurezza sulla gestione delle patch per archivi di patch alternativi.	Nota importante sulla sicurezza e best practice per l'utilizzo di repository di patch alternativi in AMS Accelerate.	10 giugno 2025
AMS Accelera la deprecazione dei record di modifica.	Il servizio AMS Accelerate Change Record diventerà obsoleto a partire dal 1° luglio 2025.	27 maggio 2025
Aggiornamenti dei sistemi operativi supportati.	I sistemi operativi supportati da AMS Accelerate vengono aggiornati, alcuni aggiunti, altri rimossi.	22 maggio 2025
Nota per i servizi supportat i nella regione del Medio Oriente (Emirati Arabi Uniti).	Supporto limitato per alcuni servizi nella regione del Medio Oriente (Emirati Arabi Uniti).	22 maggio 2025

Solo interno APIs.	Solo interni APIs che appaiono in alcuni registri. CloudWatch	22 maggio 2025
Sono state aggiunte le posizioni di registro mancanti.	Sono state aggiunte alcune posizioni di registro di Windows mancanti.	22 maggio 2025
Aggiornamenti AMS Accelerate Trusted Remediator.	Come utilizzare un nuovo parametro per personalizzare i `preconfigured-parameters` Trusted Advisor controlli in Trusted Remediator.	22 maggio 2025
Domande frequenti e aggiornamenti su AMS Accelerate Trusted Remediator.	Diversi aggiornamenti ai Trusted Advisor controlli supportati, domande frequenti su Trusted Remediator (aggiunta «Quali risorse distribuisce Trusted Remediator ai tuoi account?») e altro ancora. Vedi anche Trusted Advisor i controlli supportati da Trusted Remediator.	8 maggio 2025
Aggiornamento dei controlli di sicurezza AMS Accelerate Standard.	Aggiunti i controlli di «Condivisione dei gruppi di sicurezza».	8 maggio 2025
Accelera l'aggiornamento degli avvisi di monitoraggio.	Sono stati aggiunti avvisi aggiuntivi, oltre al nome dell'avviso aggiunto alla colonna Note.	28 aprile 2025
Accelera l'inventario delle risorse.	Il file del foglio di calcolo dell'inventario delle risorse (compresso) viene aggiornato.	24 aprile 2025

Accelera l'ubicazione dei log.	Sono state aggiunte altre posizioni di registro.	24 aprile 2025
Accelera nuovi ruoli e responsabilità (RACI) per la risposta agli incidenti di sicurezza.	RACI per la risposta agli incidenti di sicurezza.	27 marzo 2025
Accelera il nuovo avviso di riparazione automatica di Amazon RDS.	ID avviso: - 0224, si attiva quando lo storage allocato richiesto raggiunge o supera la soglia di archiviazione massima configurata.	27 marzo 2025
Accelera l'aggiornamento del modello di ruolo di Onboarding.	Il modello di ruolo di onboarding di AMS Accelerate è stato aggiornato per supportare le regioni GovCloud AWS.	25 marzo 2025
Avviso RDS per nuove riparazioni automatiche.	RDS-EVENT-0224 aggiunto.	17 marzo 2025
Nuova funzionalità Accelerate: notifiche relative agli incidenti.	È possibile AppRegistry utilizzarle per creare applicazioni e personalizzare le notifiche degli incidenti per tali applicazioni.	13 marzo 2025
Accelera l'aggiornamento alla soglia di monitoraggio degli allarmi RDS.	La soglia di allarme di utilizzo medio della CPU RDS è stata modificata dal 75% al 90%.	20 febbraio 2025
Accelera l'aggiornamento alla tabella di correzione automatica degli avvisi di AMS.	La tabella di correzione degli avvisi è stata ampliata con nuovi contenuti.	20 febbraio 2025

Nuova funzionalità Accelerate: Retain Alarms.	È possibile configurare Alarm Manager per conservare gli allarmi CloudWatch anziché eliminarli automaticamente.	20 febbraio 2025
Report self-service aggiornati con nuove opzioni di dati per la visualizzazione aggregata dei report	Sono state aggiunte opzioni di dati che includono nuovi nomi di campo:**`Admin Account ID`**, nome campo del set di dati: `aws_admin_account_id` e definizione: `Trusted AWS Organization account enabled by the customer` per i seguenti report self-service: • Rapporto sulle patch (giornaliero) • Rapporto di Backup (giornaliero) • Rapporto sull'incidente (settimanale) • Dashboard Resource Tagger • Dashboard Security Config Rules	28 gennaio 2025

Sono stati aggiunti AWS Trusted Advisor controlli aggiuntivi supportati da Trusted Remediator	I seguenti Trusted Advisor controlli sono ora supportati da Trusted Remediator:
	• Ottimizzazione dei costi
	  • c1cj39rr6v - Configurazione di interruzione del caricamento multiparte incompleta di Amazon S3
	• Sicurezza
	  • Hs4Ma3G199 - Le istanze DB RDS devono pubblicare i log in Logs CloudWatch
	  • Hs4Ma3G326 - L'impostazione di accesso pubblico a blocchi di Amazon EMR deve essere abilitata
	  • Hs4Ma3G272 - Gli utenti non devono avere accesso root alle istanze dei notebook AI SageMaker
	  • Hs4Ma3G325 - I cluster EKS dovrebbero avere la registrazione di controllo abilitata
	  • HHs4Ma3G118 - I gruppi di sicurezza VPC predefiniti non devono consentire il traffico in entrata o in uscita
	  • Hs4Ma3G127 - API Gateway REST WebSocket e la registraz
		28 gennaio 2025

ione dell'esecuzione dell'API devono essere abilitati

- Hs4Ma3G124 - Le istanze Amazon EC2 devono utilizzare Instance Metadata Service versione 2 () IMDSv2

- Tolleranza ai guasti
  - c1qf5bt013 - La scalabilità automatica dello storage nelle istanze database di Amazon RDS è disattivata
  - 7q GXs KIUw - Sistema di drenaggio della connessione Classic Load Balancer
  - c18d2gz106 - Amazon EBS non incluso nel piano AWS Backup
  - c18d2gz107 - Tabella Amazon DynamoDB non inclusa nel piano AWS Backup
  - cc18d2gz117 - Amazon EFS non incluso nel piano AWS Backup
  - c18d2gz105 - Network Load Balancer Cross Load Balancer
  - c1qf5bt026 - Il parametro Amazon RDS synchronous_commit è disattivato
  - c1qf5bt030 - Il parametro Amazon RDS innodb_fl

ush_log_at_trx_commit non è 1

- c1qf5bt031 - Il parametro sync_binlog di Amazon RDS è disattivato
- c1qf5bt036 - L'impostazione del parametro Amazon RDS innodb_default_row_format non è sicura
- c18d2gz144 - Monitoraggio dettagliato di Amazon EC2 non abilitato

- Eccellenza operativa
  - c18d2gz125 - Amazon API Gateway non registra i log di esecuzione
  - c18d2gz168 - Protezione elastica del carico non abilitata per i sistemi di bilanciamento del carico BalancingDeletion
  - c1qf5bt012 - Amazon RDS Performance Insights è disattivato
- Performance
  - c1qf5bt021 - Parametro Amazon RDS innodb_change_buffering che utilizza un valore inferiore a quello ottimale
  - c1qf5bt025 - Il parametro dell'autovacuum di Amazon RDS è disattivato

	• c1qf5bt028 - Il parametro Amazon RDS enable_indexonlyscan è disattivato • c1qf5bt029 - Il parametro Amazon RDS enable_indexscan è disattivato • c1qf5bt032 - Il parametro Amazon RDS innodb_stats_persistent è disattivato • c1qf5bt037 - Il parametro Amazon _logging è attivato RDSgeneral	
Foglio di calcolo aggiornato per l'inventario delle risorse	Foglio di calcolo aggiornato per l'inventario delle risorse.	23 gennaio 2025
Nuova funzionalità AMS: report self-service aggregati	I report self-service aggregati (SSR) offrono una visualizzazione dei report self-service esistenti aggregati a livello di organizzazione, su più account.	21 gennaio 2025
Nuova funzionalità Accelerate Patching: Patch Hooks	Usa questa funzionalità per configurare «hook» con i documenti di comando SSM per eseguire comandi a livello di sistema operativo prima o dopo l'applicazione delle patch.	16 gennaio 2025

Aggiornamento alla sezione Come funziona il monitoraggio	Sono state aggiunte informazioni su una nuova funzionalità, sulla configurazione delle notifiche di avviso per risorsa o ID di istanza, anziché per incidente.	08 gennaio 2025
Aggiornamento alla sezione Onboarding di EKS Monitoring and Incident Management	È stata aggiornata la nota sulla procedura di onboarding per chiarire quando i segnali di allarme vengono sospesi e ripresi.	19 dicembre 2024
Registro dell'account membro aggiunto a Trusted Remediator	Puoi utilizzare il registro degli account dei membri per trovare l'ID dell'account, l'iscrizione Regioni AWS e l'ora di esecuzione di ciascun account membro.	19 dicembre 2024
Prerequisiti per l'utilizzo di SSM Agent	Il contenuto sul blocco del traffico in uscita viene aggiornato.	4 dicembre 2024
L'accelerazione del monitoraggio e della gestione degli incidenti per EKS è ora supportata nella regione Asia-Pacifico (Hong Kong) Regione AWS	L'Asia Pacifico (Hong Kong) è ora supportata da Accelerate Monitoring and Incident Management for EKS	21 novembre 2024
Tabella delle offerte Operations On Demand aggiornata	I seguenti sistemi operativi sono supportati per gli aggiornamenti in loco: • Da Microsoft Windows 2016 a Microsoft Windows 2022 e versioni successive	11 novembre 2024

L'accelerazione del monitoraggio e della gestione degli incidenti per EKS è ora supportata in Africa (Città del Capo) Regione AWS.	L'Africa (Città del Capo) è ora supportata da Accelerate Monitoring and Incident Management for EKS	4 novembre 2024
Tabella delle offerte di Operations On Demand aggiornata	I seguenti sistemi operativi sono supportati per gli aggiornamenti in loco: • Da Microsoft Windows 2012 R2 a Microsoft Windows 2016 e versioni successive • Da Red Hat Enterprise Linux 7 a Red Hat Enterprise Linux 8 • Da Red Hat Enterprise Linux 8 a Red Hat Enterprise Linux 9 • Da Oracle Linux 7 a Oracle Linux 8	1 novembre 2024
Modello Quick Start aggiornato	Diagramma aggiornato, parametri del modello e file modello yaml.	28 ottobre 2024

Trusted Advisor controlli aggiunti a Trusted Remediator in AMS	I seguenti Trusted Advisor controlli sono ora disponibili in Trusted Remediator: • Z4 AUBRNSmz - Indirizzi IP elastici non associati • c18d2gz128 - Repository Amazon ECR senza policy del ciclo di vita configurato • c18d2gz138 - Ripristino DynamoDB Point-in-time • Hs4Ma3G323 - Dynamo dovrebbe avere la protezion e da cancellazione abilitata DBtables • Hs4Ma3G247 - Amazon EC2 Transit Gateway non dovrebbe accettare automaticamente le richieste di allegati VPC • Hs4Ma3G308 - I cluster Amazon DocumentDB devono avere la protezione da eliminazione abilitata • Hs4Ma3G299 - I cluster Neptune DB devono avere la protezione da eliminazi one abilitata • Hs4Ma3G306 - Le istantane e manuali dei cluster di Amazon DocumentDB non devono essere pubbliche • Hs4Ma3G109 - la convalida dei file di registro deve essere abilitata CloudTrail	25 ottobre 2024

	• Hs4Ma3G217: gli ambienti di CodeBuild progetto devono avere una registraz ione AWS Configuration4 • Hs4Ma3G158 - I documenti SSM non devono essere pubblici • Hs4Ma3G319 - I firewall Network Firewall devono avere la protezione da eliminazione abilitata	
Configurazioni supportate aggiornate	Sistemi operativi Oracle Linux supportati aggiornati a 9.0-9.3, 8.0-8.9, 7.5-7.9.	24 ottobre 2024
Nuova sezione aggiunta a Offboard da AMS Accelerate	Istruzioni su come effettuare l'offboard con le dipendenze Alarm Manager e Resource Tagger aggiunte a Offboard da AMS Accelerate.	24 ottobre 2024
La dashboard di Resource Tagger è ora disponibile.	La dashboard Resource Tagger è ora disponibile nella reportistica self-service.	26 settembre 2024
Ora puoi includere più indirizzi e-mail negli avvisi basati su tag.	Gli indirizzi e-mail multipli sono ora supportati negli avvisi basati su tag.	20 settembre 2024
I limiti di AMS Accelerate sono ora inclusi nella gestione delle patch di AMS.	I limiti di AMS Accelerate sono inclusi in Gestione delle patch: crea una finestra di manutenzi one delle patch.	30 agosto 2024

Aggiornamento AMS Accelerate Account Discovery	È stata aggiunta una nuova sezione in Account Discovery per la valutazione delle istanze Amazon EC2.	29 agosto 2024
La patch di base predefinita di AMS Accelerate è ora disponibile per i sistemi operativi Ubuntu.	La patch di base predefinita di AMS Accelerate è ora disponibile per i sistemi operativi Ubuntu.	22 agosto 2024
Aggiornamento AMS Accelerate Account Discovery	Quattro nuove chiamate AWS API sono state aggiunte alla sezione AWS CloudTrail Valutazione nella tabella di controllo operativa.	2 agosto 2024
Trusted Remediator ora supporta un controllo aggiuntivo	Trusted Remediator ora supporta il controllo di sicurezza Hs4Ma3G192: le istanze database RDS dovrebbero vietare l'accesso pubblico.	30 luglio 2024
AMS ora supporta Amazon Route 53 Resolver DNS Firewall	AMS ora supporta Amazon Route 53 Resolver DNS Firewall	30 luglio 2024
AMS Accelerate onboarding_role_minimal.zip ora contiene il codice Terraform	AMS Accelerate onboarding_role_minimal.zip ora contiene il codice Terraform.	30 luglio 2024
Dashboard delle regole di configurazione di sicurezza	Il dashboard delle regole di configurazione di sicurezza è ora disponibile nella reportistica self-service.	24 luglio 2024

AMS Accelerate ora supporta Oracle Linux 8.9, RHEL 8.10 e RHEL 9.4.	AMS Accelerate ora supporta Oracle Linux 8.9, RHEL 8.10 e RHEL 9.4.	5 luglio 2024
Aggiornamento del processo di individuazione degli account AMS Accelerate.	Il processo di individuazione degli account utilizzato per l'onboarding Account AWS su AMS Accelerate viene aggiornato.	1° luglio 2024
Trusted Remediator è ora disponibile.	Trusted Remediator, una soluzione AWS Managed Services che automatiz za la correzione dei AWS Trusted Advisor controlli, è ora disponibile.	24 giugno 2024
Eventi del firewall DNS di Amazon Route 53 Resolver in Security Incident Response.	AMS ora monitora gli eventi del firewall DNS di Amazon Route 53 Resolver in Security Incident Response	21 giugno 2024
Sistemi operativi supportati aggiornati	AMS Accelerate ora supporta AlmaLinux 8.3-8.9, 9.0-9.2 (AlmaLinux è supportato solo con l'architettura x86)	19 giugno 2024
Il limite automatico del profilo dell'istanza ora aumenta se viene soddisfatto il valore predefinito.	AMS ora aumenta il limite predefinito del profilo di istanza a 20 se viene raggiunto il limite predefinito di 10.	18 giugno 2024
La funzionalità di installazione automatica di AMS SSM Agent è ora abilitata per impostazi one predefinita.	La funzionalità di installazione automatica di AMS SSM Agent è abilitata per impostazione predefinita per gli account registrati dopo il 6/03/2024.	7 giugno 2024

Domande frequenti sulla sicurezza aggiunte alla Gestione della sicurezza.	È ora disponibile una FAQ sulla sicurezza che copre le domande più comuni sulle migliori pratiche di sicurezza, i controlli, i modelli di accesso e i meccanismi di controllo utilizzati quando un tecnico operativo o un addetto all'automazione di AMS accede agli account.	3 giugno 2024
AWS Regioni aggiuntive ora supportate da Monitoring and Incident Management for Amazon EKS.	Tre AWS regioni aggiuntive sono ora supportate da Monitoring and Incident Management for Amazon EKS.	23 maggio 2024
Le notifiche di patch relative alle richieste di assistenza vengono ora inviate prima delle finestre di manutenzione delle patch.	L'applicazione delle patch di AMS Accelerate crea una nuova richiesta di servizio 4 giorni prima della finestra di manutenzione delle patch. È possibile utilizzare la richiesta di assistenza per comunicare con AMS per apportare modifiche alla patch o per saltare una patch.	3 maggio 2024
Soglie di avviso aggiunte alla tabella degli avvisi di base di monitoraggio di AMS Accelerate EKS.	Le soglie di avviso dettagliate sono ora disponibili nella tabella degli avvisi di base per il monitoraggio di Amazon EKS.	3 maggio 2024

Aggiornato: profili di configurazione di Alarm Manager.	Sono state aggiunte note sulla creazione di allarmi di rilevamento delle anomalie con Alarm Manager.	25 aprile 2024
Aggiunte ai profili di configurazione di Resource Tagger.	Le tabelle DynamoDB e i bucket Amazon S3 sono ora disponibili in Resource Tagger	25 aprile 2024
È stata aggiunta la sezione informativa sulla gestione degli eventi pianificati (PEM).	Informazioni dettagliate sull'offerta del servizio PEM sono ora disponibili nella Guida per l'utente di AMS Accelerate.	25 aprile 2024
AMS supporta Red Hat Enterprise Linux (RHEL) 9.x.	AMS supporta Red Hat Enterprise Linux (RHEL) 9.x.	25 aprile 2024
AMS Accelerate supporta il reporting per tutte le configurazioni AWS regionali.	AMS Accelerate supporta SSM Inventory Reporting per tutte le configurazioni AWS regionali.	25 aprile 2024
Aggiornato: politiche AWS gestite.	Aggiornato il AWSManagedServicesDeploymentToolkitPolicy con nuove autorizzazioni ECR.	4 aprile 2024
Aggiornamento: sezione Resource Tagger Configuration Profiles	`AWS::EFS::FileSystem` Aggiunto all'ResourceTypeelenco.	21 marzo 2024

Aggiornato: segnalazioni di incidenti e richieste di assistenza nella sezione Accelerate.	Modificato il titolo dell'argomento in Rapporti sugli incidenti, richieste di assistenza e domande sulla fatturazione in Accelerate. È stata aggiunta una nuova sezione, Domande sulla fatturazione.	21 marzo 2024
Aggiornamento: sezione Come funziona la gestione delle richieste di assistenza.	Sono stati aggiunti chiarimenti su come AMS gestisce le richieste di servizio che contengono una richiesta di funzionalità o un bug.	21 marzo 2024
Aggiornato: crea il ruolo aws_managedservices_onboarding_role con la sezione CloudFormation	Aggiunti comandi da cui creare il ruolo. AWS CloudShell	21 marzo 2024
Aggiornato: modello Quick Start (facoltativo)	Sono stati aggiunti i comandi da cui scaricare il modello AWS CloudShell.	21 marzo 2024
Nuovi tipi di risorse disponibili per i profili di configurazione di Alarm Manager.	Aggiunti tipi di risorse per Amazon FSx, Amazon EFS ed Elasticsearch ai profili di configurazione di Alarm Manager.	21 marzo 2024
Sono disponibili sostituzioni di pseudoparametri aggiuntive per il profilo di configurazione.	Sono state aggiunte le sostituzioni di FSx pseudoparametri Amazon EFS e Amazon.	21 marzo 2024

È stata aggiunta una nuova sezione alle funzionalità nell'argomento relativo alla descrizione del servizio.	È stata aggiunta una nuova sezione, Gestione delle richieste di assistenza nelle funzionalità di AMS Accelerate.	21 marzo 2024
Nuove colonne aggiunte al rapporto settimanale sugli incidenti di segnalazione self-service	Sono state aggiunte nuove colonne al rapporto settimanale sugli incidenti in modo da poter filtrare gli incidenti in base al trimestre, al mese, alla settimana o al giorno in cui l'incidente è stato creato o risolto.	11 marzo 2024

Aggiornamenti precedenti

La tabella seguente descrive le modifiche importanti alla documentazione della guida AMS Accelerate prima di marzo 2024.

Modifica	Descrizione	Data
Miglioramenti per l'onboarding dei CloudTrail trail con AMS Accelerate	Miglioramenti per l'onboarding dei CloudTrail trail con AMS Accelerate: • Raccogli tutte le policy relative ai bucket in un unico blocco • Rimuovi il secondo ID AWS dell'organizzazione nelle dichiarazioni politiche • Chiarire i requisiti relativi all'ambiente del cliente Per ulteriori informazioni, consulta Rivedi e aggiorna le configurazioni per consentir	23 febbraio 2024

Modifica	Descrizione	Data
	e ad AMS Accelerate di utilizzare il tuo trail CloudTrail.	
Aggiornato: processo di registrazione dell'account.	È stata ristrutturata la sezione relativa alla procedura di registrazione dell'account per rendere più chiari i passaggi. È stato inoltre aggiunto un modello Quick Start opzionale per le funzionalità di onboarding. Per informazioni, consulta (Facoltativo) Modello Quick Start in Accelerate.	22 febbraio 2024
Aggiornato: Offboarding AMS Accelerate.	È stata aggiornata la sezione Considera zioni sull'offboarding di AMS Accelerate per indicare che lo `ams-access-management` CloudFormation stack e il ruolo `ams-acces s-management` IAM non vengono eliminati dal processo di offboarding. Per informazioni, consulta AMS Accelera gli effetti dell'offboarding.	22 febbraio 2024
Aggiornato: conformità alla configurazione in Accelerate.	Ove applicabile, da «Rapporto sull'incidente» è stato modificato in «Richiesta di assistenz a» per evitare confusione in merito ai presenti termini. Per informazioni, consulta Conformità della configurazione in Acceler.	22 febbraio 2024
Aggiornato: individuazione dell'account in Accelerate.	L'individuazione degli account è stata riorganiz zata in Accelerate per raggruppare meglio i prerequisiti con la sezione pertinente. Per informazioni, consulta Passaggio 1. Identificazione degli account in Accelerate.	22 febbraio 2024

Modifica	Descrizione	Data
Rinominato: AMS Patch riporta i dati alla gestione degli host AMS.	Rinominato AMS Patch Reporting in AMS Host Management e rinominato il rapporto, Patch Details report, in SSM Agent Coverage report. Per informazioni, consulta Rapporti sulla gestione degli host AMS.	22 febbraio 2024
Catalogo Operations on Demand aggiornato	È stata aggiornata la tabella delle offerte del catalogo di Operations on Demand per rimuovere i riferimenti allo «stato» in`Amazon EKS cluster maintenance` . Per informazioni, consulta Richiedere AMS Operations On Demand.	22 febbraio 2024
AMS Event Router aggiornato	È stato aggiornato il `AMSCoreRule` file nella sezione AMS Event Router. Per informazioni, consulta Utilizzo di Amazon EventBridge Managed Rules in AMS.	22 febbraio 2024
Sistemi operativi supportati aggiornati.	Sistemi operativi supportati aggiornati per includere SUSE Linux Enterprise Server 15 SP5. Per informazioni, consulta Configurazioni supportate.	22 febbraio 2024
Automazione aggiornata della correzione dell'utilizzo dei volumi EC2	È stata aggiornata la sezione dedicata all'automazione della correzione dell'utilizzo dei volumi EC2 con la corretta pianificazione dell'espansione della capacità. Per informazioni, consulta Automazione della correzione dell'utilizzo dei volumi EC2.	22 febbraio 2024

Modifica	Descrizione	Data
Aggiornato: rivedi e aggiorna le configurazioni per consentir e ad Accelerate di utilizzare il tuo trail CloudTrail	È stata aggiornata la sezione relativa alla policy sui bucket CloudTrail S3 di AMS Accelerat e Organization. Per informazioni, consultar e Rivedi e aggiorna le configurazioni per consentire ad AMS Accelerate di utilizzare il tuo trail CloudTrail.	15 febbraio 2024
Nuova funzionalità aggiunta: installazione automatica di SSM Agent	Aggiunta una nuova sezione per l'installazione automatica di SSM Agent Per informazioni, consulta Installazione automatica di SSM Agent.	26 gennaio 2024
Aggiornato: configurazioni supportate	Sono state aggiunte informazioni relative alle versioni supportate di AWS Control Tower Per informazioni, consulta Configurazioni supportate.	26 gennaio 2024
Aggiornato: segnalazione delle patch AMS.	Sono state rimosse tre sezioni dalla segnalazi one delle patch AMS: • Rapporto riassuntivo sui dettagli dell'istanza di • Rapporto sui dettagli della patch • Casi segnalati da Missed Patches Per informazioni, consulta Rapporti sulla gestione degli host AMS.	22 dicembre 2023
Aggiornato: accelera i prerequisiti per l'onboarding.	Aggiornati i piani di supporto richiesti per l'onboard di AMS Accelerate. Per informazioni, consulta Accelera i prerequis iti per l'onboarding.	15 dicembre 2023

Modifica	Descrizione	Data
Aggiornato: crea una finestra di manutenzione delle patch.	È stata rimossa la sezione predefinita del ciclo di patch poiché questa funzionalità è obsoleta. Per informazioni, consulta Creare una finestra di manutenzione delle patch in AMS.	13 dicembre 2023
Aggiornato: impostazioni di notifica in Accelerate.	È stato chiarito quale e-mail viene utilizzata per le notifiche. Per ulteriori informazioni, consulta Impostazioni di notifica in Accelerate.	12 dicembre 2023
Aggiornato: `AMSAccelerateCustomerAccessPolicies` modello.	Aggiornato il `AMSAccelerateCustomerAccessPolicies` modello per correggere un errore di sintassi. Per ulteriori informazioni, consulta Autorizzazioni per l'utilizzo delle funzionalità AMS.	12 dicembre 2023
Aggiunto: revisione della sicurezza delle richieste di modifica	È stata aggiunta una nuova sezione Modifica, richiedi revisioni di sicurezza in Gestione della sicurezza. Per ulteriori informazioni, consulta Revisioni di sicurezza delle richieste di modifica.	11 dicembre 2023
Aggiornato: resource_inventory.xlsx	È stato aggiornato il file resource_inventory.xlsx per includere i ruoli di Security Analyst. Per ulteriori informazioni, consulta Inventario risorse per Accelerate.	17 novembre 2023
Aggiornato: descrizione ams-access-admin-operations del ruolo	ams-access-admin-operationsDescrizione aggiornata. Per ulteriori informazioni, consulta Perché e quando AMS accede al tuo account e Autenticazione con identità in AMS Accelerate.	17 novembre 2023

Modifica	Descrizione	Data
Aggiornato: considerazioni sull'offboarding di AMS Accelerate	È stata aggiornata la sezione Sicurezza per chiarire cosa è disponibile su Amazon GuardDuty e AWS Config le regole dopo l'offboarding. Per ulteriori informazioni, consulta AMS Accelera gli effetti dell'offboarding.	17 novembre 2023
Aggiunto: monitoraggio e gestione degli incidenti per Amazon EKS	Il monitoraggio e la gestione degli incidenti per Amazon EKS monitora le risorse Amazon EKS per individuare guasti, peggioramento delle prestazioni e problemi di sicurezza. Per ulteriori informazioni, consulta Monitoraggio e gestione degli incidenti per Amazon EKS in AMS Accelerate.	14 novembre 2023
Aggiornato: etichettatura	Sono state aggiunte informazioni sui tag forniti dal cliente. Per ulteriori informazioni, consulta Tag forniti dal cliente in Accelerate.	7 novembre 2023
Aggiornato: profili di configurazione di Resource Tagger	Aggiunto AWS::AutoScaling::AutoScalingGroup, AWS::EKS::Cluster, AWS::Elasticsearch::Domain, and AWS::FSx::FileSystem alla sezione Filtro. Per ulteriori informazioni, consulta Profili di configurazione Resource Tagger in AMS Accelerate.	27 ottobre 2023
Aggiornato: descrizione del servizio	Aggiunto Ubuntu 22.04 ai sistemi operativi supportati. Per informazioni, consultare Descrizione del servizio.	29 settembre 2023

Modifica	Descrizione	Data
Aggiornato: prerequisiti per l'onboarding di AMS Accelerate	È stata aggiunta una nota agli endpoint VPC di AMS Accelerate per includere il modello. CloudFormation Per informazioni, consulta Accelera i prerequisiti per l'onboarding.	29 settembre 2023
Aggiornato: Detect	Tipo di protezione degli endpoint rimosso dalla risposta di sicurezza di AMS Accelerate. Per informazioni, consulta Rilevamento.	29 settembre 2023
Aggiornato: avvisi provenienti dal monitoraggio di base in AMS	Aggiunto AWS Outposts alla tabella Alerts from Baseline Monitoring. Per informazioni, consulta Rilevamento monitoring-default-metrics.	29 settembre 2023
Aggiornato: crea il ruolo aws_managedservices_onboarding_role con CloudFormation	Screenshot aggiornato per Specify Stack Details. Per informazioni, consulta Crea `aws_managedservices_onboarding_role` con CloudFormation for Accelerate.	29 settembre 2023
Aggiornamento: Amazon EventBridge Managed Rules implementato da AMS Accelerate	Aggiunta la nuova regola AMS Accelerate Amazon EventBridge Managed AMSCoreRule. AMS Accelerate Amazon EventBridge Managed Rule è stato aggiornato AMSAccess RolesRuleper aggiungere un nuovo ruolo. Per ulteriori informazioni, consulta Amazon EventBridge Managed Rules implementato da AMS.	19 settembre 2023
Aggiornato: profili di configurazione di Alarm Manager	Aggiunti gli identificatori di sostituzione degli pseudoparametri di AWS Outposts. Per informazioni, consulta Monitoraggio e gestione degli eventi in AMS Accelerate.	11 settembre 2023

Modifica	Descrizione	Data
Aggiornato: profili di configurazione Resource Tagger	Aggiunto il tipo di risorsa AWS Outposts. Per informazioni, consulta Accelera il profilo di configurazione: sostituzione di pseudoparametri.	11 settembre 2023
Aggiornato: servizi supportati	È stato aggiunto Amazon Elastic File System alla sezione Servizi monitorati dagli CloudWatch allarmi. Per ulteriori informazioni, consulta Descrizione del servizio.	6 settembre 2023
Aggiornamento: monitoraggio delle patch e correzione degli errori	È stata aggiunta la seguente nota alla sezione Utilizzo di Patch Orchestrator: «Gli avvisi di errore delle patch non vengono creati per le istanze con sistemi operativi non supportati o che vengono interrotte durante la finestra di manutenzione» Per ulteriori informazioni, consulta Comprendi la gestione delle patch in AMS Accelerate.	6 settembre 2023
Aggiornato: runbook Clarified Response to malware events	Runbook Clarified Response to malware events for Security Incident Response. Per ulteriori informazioni, consulta Risposta agli incidenti di sicurezza in AMS.	6 settembre 2023
Aggiornamento: connessione dell'account Accelerate con Transit Gateway	Passaggi chiariti per collegare un nuovo account VPC Accelerate alla rete AMS Multi-Account Landing Zone (creazione di un allegato VPC TGW): per ulteriori informazioni, consulta Collegamento dell'account Accelerate con Transit Gateway.	05 settembre 2023

Modifica	Descrizione	Data
Aggiornato: avvisi dal monitoraggio di base in AMS	È stato rimosso il riferimento a due allarmi obsoleti e. AMSRead LatencyAlarm AMSWrite LatencyAlarm Per ulteriori informazioni, consulta Avvisi dal monitoraggio di base in AMS.	05 settembre 2023
Aggiunto: AMS Event Router	È stata aggiunta la documentazione per AMS Event Router, vedere Utilizzo di Amazon EventBridge Managed Rules in AMS per ulteriori informazioni.	05 settembre 2023
Aggiornato: elenco degli pseudoparametri di Alarm Manager.	Aggiornato l'elenco degli pseudoparametri di Alarm Manager. Il parametro del nome dell'istanza EC2 è stato aggiunto alle configurazioni delle istanze EC2 e degli allarmi su disco EC2. Per ulteriori informazioni, consulta Accelera il profilo di configurazione: sostituzione di pseudoparametri.	29 agosto 2023
Aggiunto: AMS Access Offboarding	È stata aggiunta una considerazione durante l'offboarding di AMS Access. Per informazioni, consulta AMS Accelera gli effetti dell'offboarding.	24 agosto 2023
Aggiunto: AMS Security Incident Response	È stata aggiunta documentazione per l'utilizzo di AMS Security Incident Response. Per informazioni, consulta Risposta agli incidenti di sicurezza in AMS.	18 agosto 2023
Aggiornato: ruoli di accesso AMS Accelerate	È stato corretto un errore di battitura nei nomi dei ruoli. Per informazioni, consulta AWS Identity and Access Management in AMS Accelerate.	10 agosto 2023

Modifica	Descrizione	Data
Aggiornato: dichiarazioni politiche	I nomi dei ruoli codificati sono stati sostituiti con caratteri jolly. Per informazioni, consulta Rivedi e aggiorna le configurazioni per consentir e ad AMS Accelerate di utilizzare il tuo trail CloudTrail.	10 agosto 2023
Aggiornato: elenco dei servizi monitorati con avvisi EFS.	È stato aggiornato l'elenco dei servizi di monitoraggio con nuovi avvisi EFS per il monitoraggio di base AMS. Sono stati aggiunti 4 nuovi tipi di avviso EFS. Per ulteriori informazi oni, consulta Avvisi dal monitoraggio di base in AMS.	03 agosto 2023
Aggiornamento: tabella Accelerate l'inventario delle risorse	ams-backup-config-rule-stack e risorse correlate rimossi. Per informazioni, consulta Inventario risorse per Accelerate.	18 luglio 2023
Aggiornato: ruoli di accesso AMS Accelerate	<8-digit hash>Ruoli rimossi ams-backup-config-rule -st- amsBackupAlert ConfigRul e - <8-digit hash>e ams-backup-config-rule -st- amsBackupPlan ConfigRule H-. Per informazioni, consulta AWS Identity and Access Management in AMS Accelerate.	18 luglio 2023
Aggiornato: elenco degli avvisi RDS monitorati.	È stato aggiornato l'elenco degli avvisi RDS per il monitoraggio di base di AMS. Sono stati aggiunti 9 nuovi tipi di avvisi RDS e sono stati rimossi 3 tipi di avvisi RDS esistenti. Per ulteriori informazioni, consulta Avvisi dal monitoraggio di base in AMS.	19 giugno 2023
Novità: ruoli di accesso AMS Accelerate	Aggiunti nuovi ruoli di accesso per AMS Security.	16 giugno 2023

Modifica	Descrizione	Data
Novità: la gestione dei CloudTrail log di AMS Accelerate può ora utilizzare le CloudTrail tracce dei clienti.	Opzioni aggiornate supportate da Accelerat e per la gestione dei CloudTrail log, tra cui Accelerate Deployed trail o integrazione con l' CloudTrail account gestito dal cliente o l'Organization trail. Per ulteriori informazioni, consulta Rivedi e aggiorna le configurazioni per consentire ad AMS Accelerate di utilizzare il tuo trail CloudTrail.	09 giugno 2023
Aggiornato: rapporto sulla configurazione di AMS Accelerate Config Rules Response.	Rapporti aggiornati su richiesta per il AWS Config Rules Response Configuration Report. Vedi Accelerare gli aggiornamenti alla reportist ica su richiesta. Per informazioni, consulta Rapporto sulla configurazione delle risposte delle regole di configurazione di AMS Config.	26 maggio 2023
Aggiornato: Politica sulla data di inizio della fatturazione del servizio.	Definizioni aggiornate della data di inizio della fatturazione in. Termini chiave AMS	15 maggio 2023
Aggiornato: politiche AWS gestite.	L'ha aggiornato AWSManaged ServicesD eploymentToolkitPolicy con nuove autorizza zioni CFN ed ECR e ha analizzato le azioni esistenti con caratteri jolly. Vedi Accelerare gli aggiornamenti ai ruoli collegati ai servizi. Per informazioni, consulta Accelera gli aggiornam enti ai ruoli collegati ai servizi.	09 maggio 2023
Aggiornato: link alle politiche di accesso ai ruoli.	I ruoli di accesso possono ora essere scaricati direttamente dalle posizioni dei bucket Accelerate S3. Consulta Perché e quando AMS accede al tuo account e AWS Identity and Access Management in AMS Accelerate.	

Modifica	Descrizione	Data
Aggiornato: rapporto self-service sulla fatturazione mensile.	Nota aggiunta: i report di fatturazione mensile sono disponibili solo in un account Management Payer (landing zone multi-account AMS Advanced), ma sono disponibili per tutti gli account gestiti da AMS Accelerate collegati. Per informazioni, consulta Rapporto di fatturazione (mensile).	13 aprile 2023
Aggiornato: elenco degli avvisi.	CloudTrail Riferimenti rimossi. Per informazioni, consulta Gestione dei log in AMS Accelerate.	13 aprile 2023
Aggiornato: elenco degli avvisi.	Aggiunti tre nuovi avvisi per gli agenti SSM. Per informazioni, consulta Avvisi dal monitoraggio di base in AMS.	13 aprile 2023
Aggiornato: Accelerate i prerequisiti.	Ha chiarito che Accelerate richiede la presenza di uno dei quattro piani AWS Support ed esclude il piano Developer. Per informazioni, consulta Accelera i prerequisiti per l'onboarding.	13 aprile 2023
Aggiornamento: policy sui ruoli collegati ai servizi di Accelerate.	Il file zip della politica del servizio Contatti è stato aggiornato. Per informazioni, consulta AWS politiche gestite per AMS Accelerate.	13 aprile 2023
Aggiornato: AMS Resource Scheduler.	Nome del ruolo errato AWSManagedServices-DescribeScheduleOrPeriod, corretto in. AWSManagedServices-DescribeScheduleOrPeriods Per informazioni, consulta Ottimizzazione dei costi con AMS Resource Scheduler.	13 aprile 2023

Modifica	Descrizione	Data
Aggiornato: politiche AWS gestite.	Aggiornato Risposte personalizzate ai risultati con istruzioni per l'aggiornamento delle risposte personalizzate in uno o più account.	13 aprile 2023
Aggiornato: Resource Tagger	Sono stati aggiunti avvisi relativi alla «specific azione del nome per la nuova configurazione (SampleConfigurationBlock nell'esempio fornito) in quanto si potrebbe inavvertitamente sovrascrivere la configurazione gestita da AMS con lo stesso nome». Per informazioni, consulta Casi d'uso Resource Tagger in AMS Accelerate.	16 marzo 2023
Aggiornato: Patch RACI	Diversi aggiornamenti e chiarimenti al RACI per l'applicazione delle patch. Per informazioni, consulta Descrizione del servizio.	16 marzo 2023
Aggiornato: azioni nel toolkit di distribuzione SLR JSON	Politica e azioni aggiornate. Consulta Utilizzo di ruoli collegati ai servizi per AMS Accelerate.	16 marzo 2023
Aggiornato: riparazione automatica	È stato rimosso il supporto LVM per l'automaz ione dei volumi EC2. Consulta Correzione automatica degli avvisi con AMS.	16 marzo 2023
Aggiornato: Accelera l'onboard ing.	Uso chiarito dei ruoli, in particolare il ruolo minimo. Il modello per creare ruoli AMS	16 marzo 2023
Aggiornato: reportistica self-service.	I report di backup giornalieri ora supportan o le aree primarie e secondarie. Entrambi sono riportati nel campo Resource Region diRapporto di Backup (giornaliero).	16 marzo 2023

Modifica	Descrizione	Data
Aggiornato: guida all'appli cazione delle patch	È stato aggiunto un avviso che invita a non personalizzare le linee di base predefinite per l'applicazione delle patch, gestite da AMS. Create invece una nuova linea di base personalizzata per l'applicazione delle patch. Vedi: Linea di base della patch predefinita e. Patch di base personalizzate con AMS Accelerate	16 marzo 2023
Politica aggiornata sulla cessazione del servizio.	Definizioni aggiornate di cessazione del servizio e data di cessazione del servizio in. Termini chiave AMS Gli avvisi di risoluzione devono essere emessi entro il ventesimo giorno del mese precedente l'ultimo mese completo.	16 marzo 2023
Aggiornato: politiche AWS gestite.	Nome della politica chiarito:Contatta il ruolo collegato al servizio per AMS Accelerate.	16 febbraio 2023
Novità: politiche AWS gestite.	Politica aggiunta:Contatta il ruolo collegato al servizio per AMS Accelerate.	16 febbraio 2023
Aggiornato: conformità alla configurazione.	È stato corretto un errore di ortografia in:. Conformità della configurazione in Acceler	16 febbraio 2023
Nuovi contenuti: non supportat i OSes	Sono state aggiunte informazioni sui servizi forniti da AMS per i sistemi operativi non supportati (OSes), vedere. Funzionalità per sistemi operativi non supportati in Accelerate	16 febbraio 2023
Aggiornato: crea finestre di patch	È stato aggiunto un collegamento CloudShell da utilizzare perCrea una finestra di manutenzi one con l'interfaccia a riga di comando (CLI) di Systems Manager per AMS Accelerate.	16 febbraio 2023
Contenuto aggiornato: risorse per la gestione dell'onboarding	Sono stati aggiornati i modelli JSON compressi. Il modello per creare ruoli AMS	16 febbraio 2023

Modifica	Descrizione	Data
Nuovo contenuto: conformità alla configurazione	Aggiunto un nuovo argomento:Risposte personalizzate ai risultati.	16 febbraio 2023
Novità: politiche AWS gestite.	Politica aggiunta:Amazon EventBridge regola il ruolo collegato ai servizi per AMS Accelerate.	07 febbraio 2023
Aggiornato: politiche AWS gestite.	Aggiornato il `AWSManagedServices DeploymentToolkitPolicy` con nuove autorizzazioni S3. Per informazioni, consulta Accelera gli aggiornamenti ai ruoli collegati ai servizi.	30 gennaio 2023
Nuova regione di attivazione: CPT.	AMS Accelerate è ora disponibile nella regione opt-in di Capetown (CPT). Per attivare l'iscrizione, consulta Gestione. Regioni AWS	12 gennaio 2023
Aggiornato: descrizione del servizio.	Aggiunti FSx servizi monitorati dagli CloudWatch allarmi a. Descrizione del servizio	12 gennaio 2023
Aggiornato: monitoraggio delle metriche predefinite.	Aggiunti 6 FSx allarmi a. Avvisi dal monitoraggio di base in AMS	12 gennaio 2023
Aggiornato: modelli AMS.	Aggiunto Personalizza le notifiche di allarme di Cloudwatch a. Modelli AMS	12 gennaio 2023
Aggiornato: risorse per la gestione dell'onboarding.	È stata aggiornata la tabella dei modelli, aggiungendo una riga per `ams-onboarding-ssm-execution-role` in. Il modello per creare ruoli AMS	12 gennaio 2023
Aggiornato: conformità alla configurazione.	Ulteriori dettagli per richiedere riparazioni personalizzate (nella casella Importante) su. Conformità della configurazione in Acceler	12 gennaio 2023
Aggiornato: Service-linked-role autorizzazioni.	Autorizzazioni precedenti o duplicate rimosse. Per informazioni, consulta Utilizzo di ruoli collegati ai servizi per AMS Accelerate.	15 dicembre 2022

Modifica	Descrizione	Data
Aggiornato: gestione delle patch, finestre di manutenzione.	È stata aggiunta una guida alle istruzioni della console, passaggio 5, per la creazione di una finestra di manutenzione. Per informazioni, consulta Creare una finestra di manutenzione dalla console Systems Manager per AMS Accelerate.	15 dicembre 2022
Novità: sezione di gestione delle patch.	Aggiunta una sezione per le finestre di manutenzione di Patch Tuesday. Per informazioni, consulta Crea una finestra di manutenzione ricorrente «Patch Tuesday» dalla console AMS (consigliato).	15 dicembre 2022
Aggiornato: AMS Resource Scheduler.	Aggiornato il nome CloudFormation dello stack. Per informazioni, consulta Utilizzo delle risorse con AMS Resource Scheduler.	15 dicembre 2022
Aggiornato: contrassegna le tue risorse per il backup.	Sono state aggiunte linee guida per l'utilizzo di AMS Resource Tagger. Per informazioni, consulta Etichetta le tue risorse per applicare i piani di backup AMS.	15 dicembre 2022
Aggiornato: seleziona un piano di backup.	Indicato quali piani offrono un backup continuo. Per informazioni, consulta Seleziona un piano di backup AMS.	15 dicembre 2022
Aggiornato: AMS Resource Scheduler.	È stato aggiornato l'esempio AWS CLI per l'eliminazione di un periodo o di una pianificazione. Per informazioni, consulta Utilizzo di periodi e pianificazioni in AWS Managed Services Resource Scheduler.	15 dicembre 2022
Aggiornato: politiche AWS gestite.	Aggiunto il`AWSManagedServices DeploymentToolkitPolicy` . Per informazioni, consulta AWS politiche gestite per AMS Accelerate.	15 dicembre 2022

Modifica	Descrizione	Data
Novità: è stata aggiunta una sezione che descrive il nuovo ruolo AMS collegato al servizio,. AWSServiceRoleForManagedServices_DetectiveControlsConfig	GovCloud Regioni e autorizzazioni aggiunte. Per informazioni, consulta Detective controlla il ruolo collegato ai servizi per AMS Accelerate.	15 dicembre 2022
Nuova politica: AWS-gestita	È stata aggiunta una sezione che descrive come la politica AWS-managed, AWSManagedServices_AlarmManagerPermissionsBoundary, viene utilizzata nella policy sui ruoli collegati al servizio, AWSManagedServices_AlarmManager _ServiceRolePolicy, per limitare le autorizzazioni dei ruoli IAM creati dal ruolo collegato al servizio. AWSServiceRoleForManagedServices_AlarmManager Per informazioni, consulta AWS politiche gestite per AMS Accelerate.	15 dicembre 2022
Aggiornato: Operazioni su richiesta.	Offerte aggiunte: SQL Server on EC2 Operations e AMI Building and Vending. Per informazioni, consulta Operazioni su richiesta.	10 novembre 2022
Aggiornato: monitoraggio e gestione degli eventi.	Spiegazione aggiornata delle notifiche di servizio e dei report sugli incidenti. Per informazioni, consulta Come funziona il monitoraggio.	10 novembre 2022
Aggiornato: aree con ruoli collegate ai servizi	GovCloud Regioni e autorizzazioni aggiunte. Per informazioni, consulta Utilizzo di ruoli collegati ai servizi per AMS Accelerate.	10 novembre 2022

Modifica	Descrizione	Data
Novità: ruolo collegato al servizio.	Aggiunto nuovo ruolo:. `AWSServiceRoleForAMSDetectiveControls` Per informazioni, consulta Detective controlla il ruolo collegato ai servizi per AMS Accelerate.	10 novembre 2022
Aggiornato: gestione degli accessi.	Sottosezioni aggiornate con istruzioni migliorate. Per informazioni, consulta Gestione degli accessi in AMS Accelerate.	10 novembre 2022
Aggiornato: descrizione del servizio.	Pattern AMS aggiornati nella matrice RACI. Per informazioni, consulta Descrizione del servizio.	10 novembre 2022
Aggiornato: modelli AMS.	I clienti sono responsabili dell'implementazione dei pattern. Per informazioni, consulta Modelli AMS.	10 novembre 2022
Aggiornato: Offboarding.	Sono stati aggiunti dettagli su ciò che accade a specifiche risorse di Backup e Monitoraggio durante l'offboarding. Per informazioni, consulta Offboard di AMS Accelerate.	10 novembre 2022
Aggiornato: gestione delle patch..	Linee guida aggiornate e abbreviate relative alle politiche IAM. Per informazioni, consulta Creazione di un ruolo IAM per l'applicazione di patch su richiesta di AMS Accelerate.	10 novembre 2022
Novità: collegamenti ai diagrammi di architettura.	Sono stati aggiunti collegamenti ai diagrammi dell'architettura di riferimento AMS a vari argomenti. Per un esempio, consulta Monitoraggio e gestione degli eventi in AMS Accelerate.	10 novembre 2022
Novità: offerta Operations on Demand	Aggiunte «Landing Zone Accelerator Operations». Per informazioni, consulta Operazioni su richiesta.	13 ottobre 2022

Modifica	Descrizione	Data
Aggiornamento: gestione del monitoraggio. Gli avvisi generano report sugli incidenti, non richieste di assistenza	Come funziona il monitoraggio.	13 ottobre 2022
Novità: creazione di una finestra di manutenzione delle patch con un modello CFN personalizzato Accelerate	CloudFormation modelli di configurazione delle finestre di patch. Per informazioni, consulta Creare una finestra di manutenzione delle patch in AMS.	15 settembre 2022
Aggiornato: Offboarding	Ha sottolineato che i piani di backup in Accelerate non funzionano più dopo l'offboar ding. Per informazioni, consulta Offboard di AMS Accelerate.	15 settembre 2022
Aggiornato: dettagli sulla modifica CloudWatch della configurazione	È stato corretto un errore negli esempi di Windows e Linux. Per informazioni, consulta CloudWatch dettagli di modifica della configura zione.	15 settembre 2022
Aggiornato: utilizzo di AMS Resource Scheduler	Sono state aggiunte linee guida sui tag di allocazione dei costi. Per informazioni, consulta Stima dei costi in AMS Resource Scheduler.	15 settembre 2022
Aggiornamento: libreria di regole di configurazione AMS	Aggiunte due regole di `ams-eks-` configura zione alla Tabella delle regole. Per informazi oni, consulta Libreria AMS Config Rule.	15 settembre 2022
Aggiornamento: Gestione del Backup	È stata rimossa l'etichetta fuorviante PITR (point-in-time-recovery) dai titoli e dalle descrizioni dei piani di backup. Per informazi oni, consulta Seleziona un piano di backup AMS.	15 settembre 2022

Modifica	Descrizione	Data
Aggiornato: Accelerate Service Description	Descrizioni aggiornate delle regole di configurazione e dei canarini. Per informazioni, consulta Descrizione del servizio.	15 settembre 2022
Aggiornato: descrizione del servizio, configurazioni supportate	end-of-serviceData rimossa per Windows 2008 R2. Accelerate non supporta Windows 2008. Per informazioni, consulta Configurazioni supportate.	11 agosto 2022
Aggiornamento: descrizione del servizio, ruoli e responsabilità	È stata aggiornata la tabella RACI. Sono stati rimossi i registri di accesso ELB dall'ultima riga della sezione Rete. Non abilitiamo i log di accesso ELB per i clienti Accelerate. Per informazioni, consulta Ruoli e responsabilità.	11 agosto 2022
Aggiornato: conformità alla configurazione	È stato corretto un errore di battitura nella colonna Table of Rules, Frameworks. NIST-CSF era erroneamente elencato come NIST-CIS. Per informazioni, consulta Conformità della configurazione in Acceler.	11 agosto 2022
Novità: accelera l'offboarding	Considerazioni e procedure per l'offboarding. Vedi Offboarding AMS Accelerate.	11 agosto 2022
Aggiornato: elenco dei sistemi operativi degli agenti SSM preinstallati	Aggiunti «Ubuntu Linux 18.04 e 20.04" all'elenco. Per informazioni, consulta EC2 Istanze di onboarding per accelerare.	11 agosto 2022
Nuovo: Resource Scheduler	Utilizza AMS Resource Scheduler per ottimizzare i costi bloccando e avviando le risorse solo quando necessario. Per informazioni, consulta Ottimizzazione dei costi con AMS Resource Scheduler.	14 luglio 2022

Modifica	Descrizione	Data
Aggiornamento: descrizione del servizio per Resource Scheduler	Diverse sezioni della descrizione del servizio sono state aggiornate per la nuova offerta Resource Scheduler. Per informazioni, consulta Descrizione del servizio.	14 luglio 2022
Novità: AMS Patterns	AMS offre modelli di modelli, una soluzione generalizzata che risolve una famiglia di casi d'uso nell'ambiente gestito AMS. Primo modello in offerta:. Modelli AMS	14 luglio 2022
Novità: nota sull'ottimizzazione dei costi	È stata aggiunta una nota che spiega come i costi possono aumentare con l'utilizzo delle risorse. Per informazioni, consulta Inventario risorse per Accelerate.	14 luglio 2022
Aggiornamento: regole di configurazione AMS	Ha riorganizzato le tabelle in. Libreria AMS Config Rule La tabella HTML ha un numero inferiore di colonne, per facilitarne la lettura a colpo d'occhio. Il foglio di calcolo scaricabile contiene colonne aggiuntive per consentire l'ordinamento e il filtraggio.	14 luglio 2022
Aggiornato: gestione degli accessi	È stato aggiornato il CloudFormation modello di esempio inAutorizzazioni per l'utilizzo delle funzionalità AMS. La `AMSAccelerateAdminAccess` politica ora include le `IAMReadOnlyPolicy` politiche `AmsResourceSchedulerPassRolePolicy` and.	14 luglio 2022
Aggiornato: reportistica self-service	Sono state aggiunte istruzioni per crittografare i AWS Glue metadati con le chiavi KMS. Vedi la casella denominata Importante attiva. Report self-service	14 luglio 2022
Aggiornato: monitoraggio di base AMS	Aggiunto avviso DeleteRecoveryPoint di backup. Avvisi dal monitoraggio di base in AMS	14 luglio 2022

Modifica	Descrizione	Data
Aggiornato: sistemi operativi supportati	Aggiunta la data di fine del supporto per Amazon Linux 2. Descrizione del servizio	14 luglio 2022
Aggiornato: AMS Reporting	È stata aggiunta una nota sulle regioni Opt-in. Rapporti e opzioni	14 luglio 2022
Pianificatore risorse	Sono state aggiunte informazioni sull'onbo arding e sull'utilizzo di AMS Resource Scheduler per contribuire all'ottimizzazione dei costi pianificando gli orari di arresto e avvio delle risorse. Inoltre, è stata aggiornat a la descrizione del servizio Accelerate per includere la menzione di Resource Scheduler . Inoltre, è stata aggiornata la data di fine del supporto supportato da Amazon Linux 2 al 2024. Vedi Ottimizzazione dei costi con AMS Resource Scheduler e Descrizione del servizio	30 giugno 2022
Nuovo allarme	Aggiunta una AWS Backup sveglia. Avvisi dal monitoraggio di base in AMS	21 giugno 2022
Nuovo contenuto	Aggiunto il contenuto del ruolo collegato al servizio. Utilizzo di ruoli collegati ai servizi per AMS Accelerate	16 giugno 2022
	AWS Network Firewall Operations è stato aggiunto al catalogo di offerte Operations on Demand (OOD). Operazioni su richiesta	16 giugno 2022
	È stata aggiunta la descrizione della funzional ità di gestione dei problemi. Descrizione del servizio	16 giugno 2022

Modifica	Descrizione	Data
	È stata aggiunta una nota sul set di regole di configurazione che non supporta in particola ri regioni di opt-in. Conformità della configura zione in Acceler	16 giugno 2022
Contenuti aggiornati	Conformità alla configurazione. «Libreria regole AMS Config» -> «Tabella delle regole», è stata aggiornata e rimossa solo in formato ZIP. Conformità della configurazione in Acceler	16 giugno 2022
	Email di escalation rimosse. Percorso di escalation	16 giugno 2022
	L'elenco degli argomenti è stato spostato sotto i paragrafi di apertura. Cos'è AMS Accelerate?	16 giugno 2022
	Aggiornato il contenuto della meditazione automatica. Correzione automatica degli avvisi con AMS	16 giugno 2022
Contenuto aggiornato: Descrizione del servizio	È stato aggiunto EKS all'elenco dei servizi monitorati da AMS Config Rules in. Servizi supportati Descrizione del monitoraggio aggiornata nella tabella RACI in. Ruoli e responsabilità	12 maggio 2022
Contenuto aggiornato: conformità alla configurazione	Sono state aggiunte regole di configurazione relative a EKS. Per informazioni, consulta Conformità della configurazione in Acceler.	12 maggio 2022
Contenuto aggiornato: Guida introduttiva, Account Discovery	È stata aggiunta una versione più recente dello AwsAccountDiscoveryCli script (nel file zip Account Discovery Changelog) in. Passaggio 1. Identificazione degli account in Accelerate	12 maggio 2022

Modifica	Descrizione	Data
Contenuto aggiornato: monitoraggio, metriche predefinite	Condizioni di attivazione aggiornate per le metriche relative ad ALB. Per informazioni, consulta Avvisi dal monitoraggio di base in AMS.	12 maggio 2022
Contenuto aggiornato: patching onboarding	È stato aggiunto un prerequisito esplicito per l'applicazione delle patch: è necessario attivare EBS. Per informazioni, consulta Applicazione delle patch di onboarding in Accelerate.	12 maggio 2022
Contenuto aggiornato: tabella Accelera l'inventario delle risorse	ams-detective-controls-configRegole -rules-cdk modificate, regole aggiunte per ams-detective-controls-recorder -cdk e -cdk. ams-detective-controls-infrastructure Per informazioni, consulta Inventario risorse per Accelerate.	14 aprile 2022
Contenuto aggiornato: conformità alla configurazione	Introduzione agli standard di settore, alle regole di configurazione e ai tipi di risposte. Sottolinea che i clienti non scelgono regole o risposte di configurazione individuali. Conformità della configurazione in Acceler.	14 aprile 2022
Contenuto aggiornato: descrizione del servizio	È stata spostata la sezione Ambito delle modifiche esistente in Ruoli e responsabilità. Per informazioni, consulta Ruoli e responsabilità.	14 aprile 2022
Contenuto aggiornato: etichettatura e monitoraggio	Aggiunto `AWS::Synthetics:Canary` agli elenchi dei tipi di risorse consentiti per l'etichettatura e il monitoraggio. Consulta Profili di configurazione Resource Tagger in AMS Accelerate e Accelera il profilo di configurazione: sostituzione di pseudoparametri.	14 aprile 2022

Modifica	Descrizione	Data
Contenuto aggiornato: Accelerate Prerequisites	Sono state aggiunte le autorizzazioni del bucket richieste da SSM a. Amazon EC2 Systems Manager in Accelerate	14 aprile 2022
Nuovi contenuti: patch e monitoraggio	È stato aggiunto un codice di esempio per utilizzare Cloudformation per implement are configurazioni di tagging e monitorag gio. Consulta Implementazione di un profilo di configurazione con CloudFormation for Accelerate e Utilizzo CloudFormation per implementare Accelerate le modifiche alla configurazione.	10 marzo 2022
Contenuto aggiornato: console di manutenzione delle patch	Passaggi riordinati Creare una finestra di manutenzione dalla console Systems Manager per AMS Accelerate per adattarli all'interfaccia della console.	10 marzo 2022
Contenuto aggiornato: CLI di manutenzione delle patch	Parametri CLI aggiornati (pianificazione, durata e limite) per Crea una finestra di manutenzi one con l'interfaccia a riga di comando (CLI) di Systems Manager per AMS Accelerate	10 marzo 2022
Nuovi contenuti: Auto Instance Config	Aggiunta la definizione di `AMSInstan ceProfileBasePolicy` Dettagli della modifica delle autorizzazioni IAM	10 marzo 2022
Nuovi contenuti: Onboarding	È stato aggiunto un comando Linux di esempio a Connettività Internet in uscita in Accelerate	10 marzo 2022
Nuovi contenuti: onboarding	È stata aggiunta un'opzione con privilegi minimi a. Il modello per creare ruoli AMS	10 marzo 2022
Contenuto aggiornato: istruzioni per accelerare l'escalation	Sono stati aggiunti linee guida, link e contatti e-mail a Percorso di escalation	10 marzo 2022

Modifica	Descrizione	Data
Contenuto aggiornato: configurazioni supportate	AMS prevede di terminare il supporto per RHEL 6 entro il 14 CentOs marzo 2023. Per informazioni, consultare Configurazioni supportate.	10 marzo 2022
Contenuto aggiornato: tabella delle risorse	Aggiunti i ruoli IAM di accesso AMS alla tabella Inventario risorse per Accelerate delle risorse	10 marzo 2022
Contenuti aggiornati: onboarding e backup	Sono state aggiunte istruzioni per l'iscrizione a e AWS Backup Inserimento in Accelerate AWS Backup Gestione della continuità in AMS Accelerate	10 marzo 2022
Contenuto aggiornato: gestione degli accessi	Istruzioni specifiche avanzate rimosse dalla guida Accelerate. Come e quando usare l'account utente root in AMS	10 marzo 2022
Contenuto aggiornato: configurazioni supportate	AMS ora supporta Oracle Linux 8.3 e Ubuntu 18.04 e 20.04. Per informazioni, consulta Configurazioni supportate.	28 febbraio 2022
Contenuto aggiornato: Service Level Agreement	È stato aggiornato il Service Level Agreement scaricabile in. Servizi supportati	28 febbraio 2022
Contenuto aggiornato: gestione degli accessi	Aggiornato In che modo AMS accede al tuo account con FAQs i ruoli della console operatore AMS e un avviso di non modificarli o eliminarli.	28 febbraio 2022
Contenuto aggiornato: Alarm Manager	Aggiornato Accelera il profilo di configurazione: monitoraggio. Alarm Manager non è più limitato agli allarmi monometrici.	28 febbraio 2022
Contenuto aggiornato: Guida introduttiva	Aggiornato Fase 2: Risorse di gestione dell'onboarding in Accelerate. È stato aggiunto un ruolo IAM con accesso minimo alle risorse di onboarding.	28 febbraio 2022

Modifica	Descrizione	Data
Nuovi contenuti: ambito delle modifiche nella descrizione del servizio	È stata aggiunta una nuova sezione, Ambito delle modifiche apportate da AMS Accelerate che enfatizza i limiti e le azioni che AMS Accelerate non esegue.	10 febbraio 2022
Contenuto aggiornato: Guida introduttiva	Il nuovo processo di onboarding inizia con l'impostazione delle funzionalità e delle configurazioni predefinite prima della personalizzazione. Le sottosezioni contengono obiettivi specifici delle funzionalità e collegamenti correlati. Per informazioni, consulta Guida introduttiva ad AMS Accelerate.	10 febbraio 2022
Contenuto aggiornato: AMS Backup Management.	Il Gestione della continuità in AMS Accelerate capitolo è stato abbreviato e riorganizzato per motivi di leggibilità.	10 febbraio 2022
Contenuto aggiornato: etichettatura	È stata aggiunta una sezione Strumenti di etichettatura per contenere esempi di codice per CloudFormation e altri strumenti. Per informazioni, consulta Etichettatura in AMS Accelerate.	10 febbraio 2022
Contenuto aggiornato: Baseline Monitoring	Una migliore condizione di attivazione per l'allarme RedShift del cluster riduce i falsi allarmi durante la manutenzione. Per informazioni, consulta Avvisi dal monitoraggio di base in AMS.	10 febbraio 2022
Contenuto aggiornato: applicazione di patch	Comando CLI di esempio aggiornato per registrare una finestra di manutenzione. Per informazioni, consulta Crea una finestra di manutenzione con l'interfaccia a riga di comando (CLI) di Systems Manager per AMS Accelerate.	10 febbraio 2022

Modifica	Descrizione	Data
Contenuto aggiornato: AWS Config Rules Inventory.	Regola di configurazione obsoleta rimossa dalla tabella Config `ams-nist-cis-ec2-security-group-attached-to-eni` Rules Inventory. AWS Per informazioni, consulta Tabella delle regole.	27 gennaio 2022
Nuovo contenuto: creazione di finestre di manutenzione delle patch.	Aggiunto un collegamento al tutorial SSM e comandi di esempio per la creazione di finestre di manutenzione delle patch dalla riga di comando. Per informazioni, consulta Crea una finestra di manutenzione con l'interfaccia a riga di comando (CLI) di Systems Manager per AMS Accelerate.	27 gennaio 2022
Nuovi contenuti: Resource Tagger riconosce il nuovo tipo di risorsa Auto Scaling Groups (ASG).	Aggiunti i gruppi di Auto Scaling ai tipi di risorse filtrabili con i profili di configurazione Resource Tagger. Per informazioni, consulta Sintassi e struttura.	13 gennaio 2022
Nuovi contenuti: piani di backup e archivi aggiuntivi.	Sono stati aggiunti nuovi piani di backup e casseforti per mitigare gli scenari ad alto rischio, inclusi gli attacchi ransomware. Consulta Visualizza i backup nei vault AMS e Visualizza i backup nei vault AMS.	13 gennaio 2022

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.